Política de Segurança da Informação da PT Portugal a nível dos Sistemas e Tecnologias de Informação e Comunicação

Versão 2.0

Âmbito da versão 2.0:

PT Comunicações, Tmn e PT Prime. As restantes empresas, caso não tenham Políticas de Segurança da Informação próprias, poderão optar por utilizar esta Política. De qualquer das formas, quando prestarem serviços à PT Comunicações, Tmn ou PT Prime prevalece a expressa neste documento

Versão	Autor	Revisão	Data	Observações
1.0	Direcção de Gestão de Risco Técnico, Segurança e Controlo dos Sistemas de Informação (DRI)		21-12-2005	Aprovação em CE da PT Comunicações
1.0.1	Alberto Bruno (DRI/RTS) José Aser (DRI/RTS) Paula Ferreira (DRI/NCI) Pedro Inácio (DRI/RTS) Pedro Silva (DRI/PDR)	Alberto Mendes (DRI/NCI);	15-01-2007	Nova versão: 1. Alteração da classificação "*Confidencial*" do documento; 2. Introdução classificação destinatários; 3. Exclusão de cláusulas desajustadas à maturidade dos processos / Sistemas; 4. Inclusão de novas cláusulas: a) *Passwords* administração sistema;
1.1	Paula Ferreira (DRI/NCI)	José Alegria (DRI)	12-01-2008	Actualização de acordo com os comentários da DPS, DSW e Gabinete Jurídico da PT Comunicações. Actualização das referências – ISO/IEC 17799 de 2005 Simplificação, sem perda dos níveis de segurança, face à experiência com a versão 1.0
2.0	Alberto Mendes (DES/EDS) José Alegria (DES/EDS) José Aser (DES/EDS) Paula Ferreira (DES/EDS) Pedro Inácio (DES/EDS)	José Alegria (DES/EDS)	21-09-2009	Simplificação do processo de gestão de *passwords* aplicacionais. Integração das restantes empresas da PT Prime e Tmn (PTP). Actualização face a: - resultados da aplicabilidade da anterior versão; - resultados das peritagens de segurança efectuadas; - controlos definidos no âmbito SOX; - novas tecnologias na PTP.
2.1	Alberto Mendes (DES/EDS) José Alegria (DES/EDS) José Aser (DES/EDS) Paula Ferreira (DES/EDS) Pedro Inácio (DES/EDS)	José Alegria (DES/EDS)	19-02-2010	Actualização de acordo com comentários das áreas DJR, AIC, DTI, DOMM, DSE e DOI

Índice

SERVIÇO
Certif
CERTIFICADO
RDIS, PP, CA
apcer
IQNet
Serviço Fixo de Telecomunicações

PT

1 Introdução

O objectivo desta Política de Segurança da Informação é estabelecer requisitos para garantir o nível apropriado de protecção da Informação das principais empresas do Grupo Portugal Telecom que constituem a PT Portugal (PT Comunicações, Tmn e PT Prime) a nível de todos os Sistemas e Tecnologias de Informação e Comunicações, incluindo plataformas de serviços de telecomunicações, que suportam as suas operações e o seu negócio. Esta Política de Segurança da Informação abrange igualmente todos os Sistemas e Tecnologias de Informação e Comunicações, usados ou operadas por terceiros, internos ou externos ao Grupo Portugal Telecom, quando ligados directamente em rede[1] aos Sistemas e Tecnologias de Informação e Comunicações da PT Comunicações, Tmn ou PT Prime (PTP)[2].

É Política da PTP proibir acessos não autorizados, distribuição, duplicação, alteração, destruição ou apropriação indevida da informação das suas organizações. É também Política da PTP proteger a informação de entidades externas – que tenha sido confiada à PTP – de forma consistente com o seu nível de classificação, bem como em conformidade com todos os acordos, requisitos legais e normativos aplicáveis.

Pretende-se que a mesma Política conduza a PTP à aplicação de práticas mais seguras, propondo e definindo práticas mínimas, bem como caracterizando os meios e processos que observam, medem e intervêm em casos relacionados com segurança da Informação.

Para além desta Política de Segurança da Informação, deverão existir para as áreas operacionais da PTP com especificidades tecnológicas relevantes **Procedimentos Complementares de Segurança** que, sem violarem o espírito desta Política, estabeleçam os procedimentos específicos de Segurança da Informação a serem complementarmente seguidos nessas áreas operacionais.

A presente Política deverá ser aplicada, também (i) às entidades externas *(prestadoras de serviços)* a quem a PTP adjudica serviços, sempre que estas trabalhem directamente sobre sistemas e tecnologias da PTP ou tenham os seus sistemas e tecnologias ligados directamente em rede[2] com os sistemas e tecnologias da PTP, bem como (ii) ao administrador do sistema e (iii) qualquer outra pessoa ou entidade com acesso aos sistemas e tecnologias da PTP e (iv) a outras sociedades do Grupo PT que integrem ou se encontrem ligadas aos sistemas e tecnologias da PTP.

---

[1] Por "*ligados directamente em rede*" queremos dizer ligados através de interfaces de rede em que não seja possível garantir antecipadamente, de forma permanente, e com 100% de certeza, a segregação absoluta entre os sistemas e tecnologias que acedem e os sistemas e tecnologias acedidos e que suportam as operações e o negócio da PT Comunicações, Tmn ou PT Prime.

[2] No decorrer deste documento usaremos a sigla **PTP** como representando o seguinte conjunto das empresas da PT Portugal do Grupo Portugal Telecom: **PT Comunicações**, **Tmn** e **PT Prime**.

A presente Política deverá ser disponibilizada previamente às pessoas e entidades referidas no parágrafo anterior, pela pessoa responsável na PTP pela relação com a pessoa ou entidade em causa.

No âmbito da PTP:

- A entidade responsável pela Política de Segurança da Informação, referenciada ao longo deste documento, corresponde ao Departamento EDS (Eficiência, Disponibilidade e Segurança) da DES (Direcção de Exploração e Operação de SI's;

- A entidade responsável pela concepção, operacionalização e gestão dos serviços de TI's e redes corporativas da PT Portugal é a DTI (Direcção de Serviços e Tecnologias Informação) que é também responsável pela segurança operacional de todas as TI's e serviços corporativos sob sua gestão[3];

- A entidade responsável pelo desenvolvimento dos SI's da PT Portugal é a DDS (Direcção de Desenvolvimento de Sistemas de Informação) que é também responsável por assegurar que todos os novos projectos de SI's cumprem o determinado nesta Política de Segurança da Informação;

- A entidade responsável pela exploração e operação dos SI's da PT Portugal é a DES (Direcção de Exploração e Operação de Sistemas de Informação) que, através do seu Departamento EDS, é também responsável pelo controlo da segurança da informação e dos SI's em exploração;

- As entidades responsáveis pela construção da Rede da PT Portugal são a DPL (Direcção de Planeamento e Implementação da Rede) na rede core, a DSE (Direcção de Serviços Especializados ao Cliente) nas redes de clientes empresariais e a DOI (Direcção de Operações de Cliente e Infra-Estruturas) na rede de acesso e clientes residenciais; Estas entidades são também responsáveis por assegurar que todos os seus novos projectos cumprem o determinado nesta Política de Segurança da Informação;

- A entidade responsável pelo desenvolvimento de plataformas de serviço de telecomunicações da Rede da PT Portugal é a DPT (Direcção de Plataformas e Engenharia de Serviços); Esta entidade é também responsável por assegurar que todos os seus novos projectos cumprem o determinado nesta Política de Segurança da Informação;

- As entidades responsáveis pela operação e manutenção da Rede da PT Portugal são a DOMF (Direcção de Operação e Manutenção da rede *Wireline*) para a rede *Wireline* e a DOMM (Direcção de Operação e Manutenção da rede *Wireless*) para a rede *Wireless*; Estas entidades são também responsáveis por assegurar controlos

---

[3] Por exemplo, plataforma e-mail, acesso à internet, backups, etc.

de segurança da informação ao nível das redes e serviços sob sua responsabilidade;

- A entidade responsável pela tecnologia, engenharia, operação e segurança do Portal Sapo da PT Portugal é a DTS (Direcção de Tecnologia do Portal Sapo);

2 Referências

A referência aos diplomas seguidamente indicados incluem a referência às alterações aos mesmos que eventualmente tenham ou venham a ser efectuadas.

ISO / IEC 27001:2005 – Information Security Management Systems – Requirements;

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management;

Directiva 95/46 DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de Outubro de 1995 - Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

Directiva 2002/58/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 12 de Julho de 2002. - Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)

Lei 67/98 de 26 de Outubro – Lei da Protecção de Dados Pessoais;

Lei 41/2004 de 18 de Agosto – Lei relativa ao tratamento de Dados Pessoais e Protecção da Privacidade no Sector das Comunicações Electrónicas;

Decreto-Lei n.º 122/2000 de 4 de Julho - Protecção Jurídica das Bases de Dados;

Decreto-Lei nº 134/2009, de 2 de Junho - estabelece o regime jurídico aplicável à prestação de serviços de promoção, informação e apoio aos consumidores e utentes através de centros telefónicos de relacionamento (Call Centers);

Lei n.º 109/2009 de 15 de Setembro - Lei do *Ciber Crime*;

Decreto-lei n.º 252/94 de 20 de Outubro - Protecção Jurídica de Programas de Computador;

Decreto-lei n.º 290-D/99, republicado pelo Decreto-Lei n.º 62/2003, de 3 de Abril - Regime Jurídico das Assinaturas Electrónicas;

Decreto-lei n.º 7/2004 de 7 de Janeiro - Comércio Electrónico;

Decreto-Lei nº 256/2003 de 21 de Outubro - Facturação Electrónica;

Lei nº 7/2009, de 12 de Fevereiro - Código do Trabalho;

Lei *Sarbanes–Oxley Act* de Julho 2002;

Código do Direito de Autor e dos Direitos Conexos;

Código da Propriedade Industrial;

Resolução do Concelho de Ministros nº. 37/89 - Normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação (SEGNAC 2);

Resolução do Concelho de Ministros nº. 5/90 - Normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática (SEGNAC 4);

Ordem de Serviço 001403CE (PT SGPS) – Matérias Classificadas PT, Preparação, Manuseamento, Arquivo e Destruição. Entrada em vigor em de 01.08.2003;

Ordem de Serviço 001705CEPTC (PT Comunicações) – Matérias Classificadas PT, Preparação, Manuseamento, Arquivo e Destruição. Entrada em vigor em de 30.03.2005;

Ordem de Serviço OS001403CE (Tmn) - alinhamento com as directivas do Grupo PT, nomeadamente com a ordem de serviço emitida a 01/08/2003 que introduz o nível "*Muito Secreto*" e estabelece algumas regras de preparação, manuseamento, arquivo e destruição de Informação classificada;

Ordem de Serviço OS002303CE – Política Corporativa de Segurança de Sistemas de Informação da PT Comunicações;

Ordem de Serviço OS001108CE de 17-07-2008 PT SGPS – Princípios a observar no modelo de gestão de acessos das empresas do Grupo PT.

3 Âmbito

A Política de Segurança da Informação aqui descrita é aplicável a todos os funcionários, fornecedores, consultores, incluindo os colaboradores de entidades externas ou outras entidades e/ou pessoas que acedam aos Sistemas e Tecnologias de Informação e Comunicações da PTP, pelo que a todos deverá ser disponibilizada. Nesta Política de Segurança da Informação, o termo "*utilizadores*" será utilizado como referência a qualquer um dos indivíduos atrás referidos.

É indispensável assegurar que todos os Utilizadores, independentemente do seu nível hierárquico, função e/ou vínculo contratual – internos à PTP ou afectos a entidades externas ou outros com quem a PTP contratou um fornecimento de Produtos/Serviços – têm conhecimento desta politica e acesso adequado à informação necessária para o desempenho das suas funções, sendo exigido destes o respeito pelos controlos de segurança implementados e o cumprimento dos seguintes valores:

- **Integridade** – prevenção contra a modificação e/ou destruição não autorizada de Informação, salvaguardando a respectiva fiabilidade e origem;
- **Confidencialidade** – prevenção contra o acesso e/ou divulgação não autorizados de Informação;
- **Disponibilidade** – garantia do acesso autorizado à Informação sempre e na medida do necessário.

A segurança da informação, ou seja a sua confidencialidade, integridade e disponibilidade, é uma responsabilidade de todos.

O conteúdo da Política de Segurança da Informação destinado exclusivamente aos **Utilizadores das Áreas Técnicas** (por exemplo, das áreas de Sistemas de Informação e Infra-estruturas Tecnológicas, Planeamento, Engenharia e Operações de Serviços de Rede) da PTP, ou de entidades externas com responsabilidades técnicas, encontra-se classificado com o seguinte símbolo:

A Política aqui descrita é aplicável a todos os Sistemas e Tecnologias de Informação e Comunicação da PTP (**OSS** e **BSS**), bem como à comunicação entre estes.

A aplicação desta Política deverá no entanto ser efectuada de forma diferenciada de acordo com a seguinte classificação dos Sistemas e Tecnologias de Informação e Comunicação:

- **Novos sistemas e tecnologias[4];**
- **Sistemas e tecnologias já existentes e incluídos no âmbito SOX;**
- **Sistemas e tecnologias já existentes e não incluídos no âmbito SOX.**

3.1 Novos Sistemas e Tecnologias de Informação e Comunicação

Para os novos Sistemas e Tecnologias de Informação e Comunicação da PTP deverá ser garantido o cumprimento integral da Política aqui definida, devendo este requisito ser assegurado desde o momento de procura e selecção da solução tecnológica a adoptar, logo durante a fase de selecção e negociação com os possíveis fornecedores, pelo que aos mesmo deverá ser disponibilizada, ao abrigo de cláusula de confidencialidade, nos termos dos parágrafos seguintes.

O Cliente interno é responsável por, aquando da elaboração de documentos para Consulta ao Mercado, como por exemplo o Caderno de Encargos, RFI, RFP ou RPQ, incluir as seguintes cláusulas[5]:

Cláusula de Confidencialidade e Protecção de Dados Pessoais

1. Os concorrentes obrigam-se a manter e tratar como absolutamente confidencial toda a informação trocada no âmbito da presente consulta, abstendo-se de qualquer uso fora deste contexto, quer em benefício próprio, quer de terceiro, independentemente dos fins, salvo:
   a) Em situações de litígio entre a Entidade Adjudicante e o concorrente, caso em que a informação relevante poderá ser apresentada perante a autoridade competente;
   b) Quando a informação em causa for solicitada por uma autoridade pública com poderes para o requerer, devendo dessa solicitação o concorrente dar conhecimento de imediato à Entidade Adjudicante.
2. A obrigação prevista no número anterior manter-se-á por um período de 3 (três) anos a contar da data de abertura do presente procedimento.
3. Os concorrentes são responsáveis por todos e quaisquer danos decorrentes do incumprimento culposo ou negligente das obrigações referidas em 1. e 2. relativamente ao uso das informações trocadas, assim como pela confidencialidade e utilização da informação supra referida por parte dos respectivos colaboradores que a ela, a qualquer título, tenham acesso.
4. Os concorrentes obrigam-se ainda a cumprir a legislação em vigor sobre Protecção de Dados Pessoais, nomeadamente, nos termos do disposto na Lei n.º 67/98, de 26 de Outubro relativa à protecção de dados pessoais

[4] Todos os sistemas e tecnologias de informação e comunicação instalados após a data de aprovação deste documento
[5] Os textos deverão ser transcritos na íntegra, pelo que não devem ser alterados.

e/ou na Lei 41/2004, de 18 de Agosto, relativa ao tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas se, no âmbito da prestação de serviços objecto da presente consulta, vierem a ter acesso aos mesmos.

Cláusula de Conformidade com a "*Política de Segurança da Informação da PT Portugal a nível dos Sistemas e Tecnologias de Informação e Comunicação*"

Os concorrentes obrigam-se a garantir que os Produtos/Serviços a serem fornecidos no âmbito da presente consulta ao mercado estão em conformidade com a ***"Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações"***, incluída em anexo, cujo conteúdo se encontra sujeito a obrigação de confidencialidade.

O Cliente interno deverá incluir como anexo ao documento para Consulta ao Mercado a ***"Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações"***.

Na contratação de um produto/serviço, o Cliente interno deverá salvaguardar que, a proposta apresentada pelo fornecedor refere expressamente, por escrito, que os Produtos/Serviços a serem contratados estão em conformidade com a ***"Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações"*** e que estão explicitamente reflectidas nessa proposta as cláusulas de confidencialidade e protecção de dados pessoais constantes desta Política de Segurança da Informação, sendo o fornecedor responsável pelos danos decorrentes para a PTP e/ou terceiros pela violação da presente Política por parte do fornecedor e/ou seus colaboradores, agentes e/ou subcontratados.

Após a adjudicação, o Cliente interno da PTP deverá:

- Garantir que todos os desenvolvimentos têm por base as boas práticas de desenvolvimento de software, reconhecidas internacionalmente em matéria de segurança, de forma a evitar-se a ocorrência de erros comuns e de vulnerabilidades de segurança conhecidas;
- Garantir segundo um plano de testes especificamente desenhado para as conformidades de segurança da informação, que antes dos novos sistemas ou tecnologias da informação ou comunicação entrarem em produção, são efectuados testes específicos relativamente aos mesmos;
- Garantir que antes dos novos sistemas ou tecnologias da informação ou comunicação entrarem em produção, estes estão em conformidade com a "*Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações*";

- Garantir que qualquer fornecedor da PTP, antes do início do fornecimento de um Produto/Serviço, que implique o acesso a sistemas e tecnologias de informação ou de comunicação da PTP, assina um Acordo de Confidencialidade *(NDA*[6] *– Non Disclosure Agreement)* que garanta o cumprimento desta Política de Segurança da Informação para além de outras disposições específicas ao fornecimento em causa.

3.2 Sistemas e Tecnologias já Existentes e Incluídos no Âmbito SOX

Para os sistemas e tecnologias nestas condições, deverão ser implementadas de imediato as alterações necessárias para garantir o cumprimento integral da Política aqui definida, excepto quando forem identificadas razões técnicas ou de negócio que inviabilizem a implementação das alterações referidas.

As excepções identificadas deverão ser documentadas e sujeitas a parecer da entidade responsável pela Política de Segurança da Informação, acompanhada de proposta de medidas que possam, entretanto, mitigar os riscos em causa (para mais detalhe ver ponto 8.2).

3.3 Sistemas e Tecnologias já Existentes mas Não Incluídos no Âmbito SOX

Para os sistemas e tecnologias nestas condições, é assumido o não cumprimento integral da Política aqui definida, devendo no entanto, existir um plano de mitigação ou de correcção das partes em incumprimento.

Estes casos deverão ser identificados como excepções e devem ser devidamente documentados. Sempre que uma acção de renovação tecnológica não conduza ao cumprimento integral da "*Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações*", deverá ser mantida a identificação deste sistema como uma excepção documentada, salvaguardando que nenhuma alteração possa conduzir a uma situação de risco acrescido de segurança comparativamente à situação anterior.

A responsabilidade pela documentação do incumprimento que levou à excepção deverá caber à equipa responsável por esse sistema ou tecnologia de informação e comunicações. (para mais detalhe ver ponto 8.3).

---

[6] De acordo com minuta a solicitar à Direcção Jurídica

4 Responsabilidades Gerais

4.1 Responsabilidades Gerais dos Utilizadores

Os equipamentos informáticos disponibilizados pela PTP aos Utilizadores destinam-se ao exercício da respectiva actividade profissional, devendo os Utilizadores zelar pela sua boa conservação e utilização adequada. É da responsabilidade do Utilizador a salvaguarda da sua informação pessoal e garantir que esta não é legalmente ilícita ou imprópria face ao código de ética da PT.

Os colaboradores da PTP, enquanto Utilizadores do software disponibilizado pela PTP, deverão cumprir integralmente os termos e condições de utilização do software.

Um colaborador da PTP que cometa uma violação à presente Política, através do incumprimento das disposições descritas neste documento, estará sujeito ao disposto na Lei Geral de Trabalho, designadamente no que respeita ao seu sancionamento disciplinar ou, no caso de ser colaborador com vínculo contratual com a PT Comunicações, estará sujeito ao disposto no Acordo de Empresa em vigor, igualmente e designadamente no que respeita ao poder disciplinar.

4.2 Responsabilidades gerais de entidades externas

Os equipamentos informáticos disponibilizados pela PTP aos Utilizadores externos destinam-se à execução do serviço contratado, devendo estes Utilizadores zelar pela sua boa conservação e utilização adequada. É da responsabilidade do Utilizador a salvaguarda da sua informação pessoal e garantir que esta não é ilícita ou imprópria face ao código de ética da PT.

Os colaboradores externos da PTP, enquanto Utilizadores do software disponibilizado pela PTP, deverão cumprir integralmente os termos e condições de utilização do *software*.

Caso se verifique uma violação à presente Política, através do incumprimento das disposições descritas neste documento, por parte de fornecedores, consultores ou colaboradores de entidades externas que acedem aos Sistemas e Tecnologias de Informação e Comunicação da PTP, poderá proceder-se a uma acção legal e despoletar as penalizações previstas nos contratos existentes entre a PTP e a entidade em causa, bem como recorrer aos outros mecanismos previstos na lei, sendo ainda imediatamente revogados todos os direitos de acesso aos sistemas e tecnologias da PTP por parte do elemento incumpridor. Para o efeito, deverá ser alterada a respectiva *password* de acesso aos sistemas e desactivado o respectivo acesso às instalações da PTP.

4.3 Responsabilidades gerais das chefias e das áreas de gestão dos recursos humanos

Sempre que exista uma alteração significativa de responsabilidades ou funções de um Utilizador a respectiva chefia deverá informar a área responsável pela Gestão de Utilizadores para que possam ser alterados os respectivos privilégios do Utilizador.

Sempre que termine a colaboração de um funcionário PTP, a área de recursos humanos deverá informar as áreas responsáveis pela Gestão de Utilizadores para que esse colaborador possa ser, o mais rapidamente possível, desactivado e os seus acessos cancelados em todas as redes, sistemas de informação, plataformas tecnológicas, e pontos de acesso físico aos edifícios PT. A área de gestão de recursos humanos deverá também garantir a recolha do cartão de empregado assim como a eliminação de toda a informação de carácter biométrico associado a esse funcionário. Caso o funcionário tenha um nível hierárquico com responsabilidades de gestão ou tenha, dentro das suas funções, lidado com informação confidencial, toda a informação no seu Desktop e/ou Notebook deverá ser destruída antes que este seja reaproveitado para outro utilizador.

Sempre que termine a colaboração de um funcionário de uma entidade externa, a área na qual desenvolveu a sua actividade deverá informar as áreas responsáveis pela Gestão de Utilizadores para que possa ser, o mais rapidamente possível, desactivado e os seus acessos cancelados em todas as redes, sistemas de informação, plataformas tecnológicas, e pontos de acesso físico aos edifícios PTP. A área interna responsável pelo serviço prestado pela entidade externa, deverá também assegurar a recolha de eventuais cartões de acesso assim como a eliminação de toda a informação de carácter biométrico associado a esse funcionário externo. Caso esse funcionário externo tenha, dentro das suas funções, lidado com informação confidencial, toda a informação no seu Desktop e/ou Notebook deverá ser destruída antes que este seja reaproveitado para outro utilizador.

Em circunstância alguma dever-se-ão permitir Desktops ou Notebooks ligados à rede interna sem que estes tenham Utilizadores autorizados.

5 Comunicação e Gestão da Informação

5.1 Classificação de Informação

Os graus de classificação de segurança da informação, correspondentes ao nível de sensibilidade da informação, definidos na empresa são os seguintes[7]:

PT Muito Secreto – O grau de classificação **PT Muito Secreto** é limitado a informações, documentos e materiais que necessitem do mais elevado grau de

[7] Ordem de Serviço 001403CE (PT SGPS) – Matérias Classificadas PT, Preparação, Manuseamento, Arquivo e Destruição. Entrada em vigor em de 01.08.2003

protecção. Deve ser aplicado unicamente a matérias cujo conhecimento, ou a divulgação por pessoas não autorizadas para tal, possa implicar consequências excepcionalmente graves para a PTP ou para uma das suas Empresas participadas.

São exemplos de matérias a classificar de **PT Muito Secreto** as que constem de directivas, planos ou ordens estratégicas a nível de administração das Empresas.

PT Secreto – Este grau de classificação aplica-se a matérias cujo conhecimento ou a divulgação por pessoas não autorizadas para tal, possa implicar consequências graves para a PTP ou para uma das suas Empresas participadas.

São exemplos de matérias a classificar de **PT Secreto** as que constem de estudos e documentos sobre o fornecimento de novas soluções tecnológicas ou aperfeiçoamentos considerados estratégicos para o negócio das Telecomunicações, ou outras circunstâncias que denunciem questões altamente sensíveis para a PTP.

PT Confidencial – Este grau de classificação aplica-se a matérias cujo conhecimento, ou a divulgação por pessoas não autorizadas para tal, pode ser prejudicial para a PTP ou para uma das suas Empresas participadas.

São exemplos de matérias a classificar de PT Confidencial as que constem de:

- Documentos ou informação operacional, técnica ou comercial que possa conter informação útil à concorrência;
- Informações ou estudos sobre grandes clientes ou segmentos de mercado que possam conter informação útil à concorrência;
- Ficheiros com dados pessoais de clientes ou de outras pessoas singulares;
- Processos de natureza pessoal ou disciplinar.

PT Reservado – Este grau de classificação é aplicado a matérias limitadas a uso departamental que, embora não requerendo classificação mais elevada, não devem ser do conhecimento de pessoas que delas não necessitem para o estrito cumprimento das suas funções.

São exemplos de matérias a classificar de **PT Reservado**:

- Informações referentes a aos colaboradores;
- Textos técnicos cujo conteúdo exija protecção no interesse das Empresas;
- Informação de firmas ou organizações, relativas a ofertas, propostas ou transacções cujo conhecimento indevido possa prejudicar ou favorecer indevidamente terceiros.

O grau de classificação de segurança atribuído a uma matéria/documento não deve ser nem superior nem inferior ao requerido pela matéria em análise.

A atribuição do grau de classificação **PT Muito Secreto** compete exclusivamente aos membros da Comissão Executiva ou, quando não haja, do Conselho de Administração ou do Conselho Gerência, consoante os casos, não podendo, em caso algum, ser subdelegada.

A atribuição do grau de classificação **PT Secreto** compete aos membros da Comissão Executiva ou, quando esta não exista, aos membros do Conselho de Administração ou do Conselho de Gerência, consoante os casos, ou ainda aos Directores das Empresas.

A atribuição dos graus de segurança **PT Reservado** e **PT Confidencial** compete aos funcionários que assinarem o documento ou informação cuja segurança se deseja garantir, tendo em consideração as regras e a necessidade atrás definidas.

Os ficheiros classificados como Muito Secreto, Secreto ou Confidencial armazenados em bases de dados ou ficheiros do sistema devem ser cifrados, de forma a evitar a sua consulta por parte da equipa técnica de operação e manutenção, outros Utilizadores privilegiados ou através de acessos não autorizados.

A informação classificada como PT Confidencial ou PT Reservada não deverá ser reencaminhada a não ser que tal seja mesmo necessário e crítico para o negócio e a mensagem e respectivos anexos estejam cifrados.

As instalações da PTP que contenham informação classificada como PT Muito Secreto e PT Secreto deverão assegurar mecanismos de controlo de entrada acrescidos (tais como cartões de identificação, restrição de acesso aos pisos, detecção de impressão digital por via óptica ou outros meios biométricos), de forma a identificar, autenticar e registar as entradas e deslocações.

A não classificação expressa de informação como Classificada não obsta a que a mesma deva ser considerada como tal, em função do seu conteúdo. Na dúvida quanto ao grau de classificação de determinada informação, deverá ser a mesma considerada como sujeita à mais segura das que se considerarem mais adequadas.

A informação de domínio Público deverá ser expressamente classificada como PT Público.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

7.2 Information Classification

5.2 Gestão de Meios Amovíveis

5.2.1 Utilização de Meios Amovíveis

As drives para meios amovíveis nomeadamente, "*USB pens*", Discos externos, CDs, DVD's, Tapes, etc., não deverão estar disponíveis nas Estações de Trabalho (ET) quando não houver uma razão de negócio que o justifique.

Cabe ao Director de cada área a identificação e autorização das ET para as quais deverão ser indisponibilizadas as drives para os meios amovíveis.

Deve no entanto ser garantido que não são disponibilizadas ou permitidas drives para meios amovíveis no caso das Estações de Trabalho de risco (ver 6.8.2).

É estritamente proibida a execução de software não autorizado a partir de qualquer meio amovível.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.7 Media handling

5.2.2 Transporte de Informação Classificada

Sempre que seja necessário efectuar o transporte de um documento ou qualquer meio amovível, "*USB pens*", Discos externos, CDs, DVD's, Tapes, etc com informação classificada deverão ser garantidas todas as medidas necessárias para proteger a confidencialidade, integridade e disponibilidade antes, durante, e depois do transporte. A informação constante dos meios amovíveis a utilizar deverá ser cifrada previamente ao transporte.

O transporte de informação classificada será feito sempre por Utilizadores autorizados para o efeito.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.7 Media handling

5.3 Eliminação de Informação

5.3.1 Eliminação de Documentos Classificados

Devem ser destruídos periodicamente, e logo que conveniente, todos os documentos já substituídos ou caducados, salvo no caso de matérias classificadas como **PT Muito Secreto** em relação às quais a destruição apenas será feita após solicitação ao arquivo pela entidade emissora.

Sempre que o detentor de matéria ou documento classificado de **PT Muito Secreto** entenda que o mesmo se tornou inútil deve propor à entidade emissora que proceda ou mande proceder à sua destruição. Os serviços responsáveis pelo arquivo de matérias classificadas não necessitam de aguardar instruções para procederem à destruição de rotina de documentos classificados.

De qualquer modo, o bom senso, a racionalidade económica e a segurança devem presidir à decisão da oportunidade da destruição. Em regra, deve evitar-se a

manutenção em arquivo de documentos classificados com mais de 5 anos, cujo interesse histórico não seja reconhecido, ou que se tenham tornado desnecessários.

Na destruição de rotina de documentos classificados devem ser usadas máquinas trituradoras, retalhadores ou incineradores que garantam eficazmente a inutilização efectiva da informação neles contidos.

Deverá ser sempre considerado o tempo de retenção definido para cada tipo de informação antes de avançar com a sua eliminação, nomeadamente verificar o período de conservação da documentação e do tipo de dados, nos termos previstos na lei aplicável, designadamente em matéria contabilística e fiscal e nas legalizações notificadas à Comissão Nacional de Protecção de Dados.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.7.2 Disposal of media

5.3.2 Eliminação de Media

Todos os CDs/DVD's, discos magnéticos, bandas/cartridges magnéticas, etc que já não sejam necessários devem ser fisicamente destruídos ou colocados em recipientes adequados para que sejam posteriormente destruídos por uma empresa devidamente certificada para o efeito. O processo de destruição física deverá impossibilitar qualquer recuperação de informação mesmo que parcial. Esta destruição deverá ser sempre devidamente acompanhada por um quadro autorizado da PTP e após verificação do período de conservação do tipo de dados, nos termos previstos na lei aplicável, designadamente em matéria contabilística e fiscal e nas legalizações notificadas à Comissão Nacional de Protecção de Dados.

Sempre que termine a colaboração de um funcionário (interno ou de uma entidade externa) a respectiva chefia deverá informar a área responsável pela Gestão de Equipamentos para que possam ser eliminados os registos de informação desse colaborador com meio adequado à confidencialidade da informação relativa à função desempenhada.

É da responsabilidade do funcionário (interno ou de uma entidade externa) com o qual terminou a colaboração a salvaguarda da sua informação pessoal.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.7.2 Disposal of media

5.3.3 Retenção e Eliminação de Informação Histórica

Devem ser estritamente garantidos os prazos de retenção para os diferentes tipos de informação de acordo com as diferentes leis a que a PTP está obrigada.

Por outro lado, é uma medida básica de segurança e de racionalidade económica não manter informação que já não seja de utilidade prática e que já não tenha de ser retida por obrigações legais ou regulamentares externas (CNPD, SOX, Tribunais, Autoridades Policiais, etc.). Informação histórica que apenas tenha de ser retida por razões judiciais deverá ser mantida à guarda reservada da Direcção Jurídica que deverá depois garantir a sua eliminação quando esta informação deixar de ser necessária.

Em particular, emails, audit trails, logs aplicacionais e de sistema e toda e qualquer outra informação não essencial após o seu período de utilidade legal e prática deverá ser eliminada dos sistemas e arquivos de dados (discos e outros meios magnéticos). Assim, os prazos máximos de retenção de informação não abrangida por leis ou regulamentos externos deverão ser determinados por Ordem de Serviço específica.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10. Communications and operations management

5.4 Armazenamento de Informação

5.4.1 Armazenamento de Informação em Servidores

Todos os servidores com informação relevante da PTP terão de estar alojados em *Data Center* sob a responsabilidade de uma entidade operacional reconhecida que assegure a sua administração de sistemas e a sua segurança física e lógica dentro das melhores práticas e do disposto na presente Política.

Sempre que um servidor deixe de ser utilizado deve ser imediatamente desligado da rede e a sua informação destruída após verificação do período de conservação do tipo de dados, nos termos previstos na lei aplicável, designadamente em matéria contabilística e fiscal e nas legalizações notificadas à Comissão Nacional de Protecção de Dados. No caso excepcional em que este servidor tenha de ser mantido mais algum tempo ligado à rede, será obrigatório garantir a sua segurança lógica através da eliminação de todos os acessos lógicos desnecessários para impedir a sua utilização como base de ataque informático.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

9.2 Equipment security

5.4.2 Gestão e Utilização da Documentação de Sistemas e Tecnologias de Informação e Comunicação

A documentação relativa aos sistemas e tecnologias de informação e comunicação da organização (exemplo, manuais operacionais e de utilização) deverá estar actualizada e acessível apenas a quem for autorizado, nomeadamente equipas de suporte e manutenção.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.7.4 Security of system documentation

5.5 Comunicação de Informação

As regras constantes desta Política relativas à utilização das ferramentas electrónicas disponibilizadas pela PTP, não dispensam a consulta do Regulamento Interno da PTC e TMN acerca da utilização de e-mail, fax, telefone, telemóvel, acesso à Internet, bem como as ordens de serviço com este relacionadas.

5.5.1 Informação Classificada como PT Muito Secreto ou PT Secreto

Não é permitida a transmissão por meios electrónicos de qualquer tipo (incluindo assim e-mail, fax, telefone, telemóvel e Internet) de matéria ou documento classificado como **PT Muito Secreto** ou **PT Secreto**, ainda que parcial.

5.5.2 Utilização de FAX

Informação **PT Confidencial** ou **PT Reservada** apenas poderá ser enviada por fax se não for possível efectuar a transmissão por meios mais seguros. O emissor da informação e o destinatário deverão aprovar a respectiva transmissão previamente, que, pelo menos quanto a informação **PT Confidencial**, deve ser acompanhada de comunicação paralela para o destinatário, de forma a assegurar que a informação chegou aos eu destinatário.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.8 Exchange of Information

5.5.3 Utilização de Impressoras

Informação classificada como **PT Confidencial** ou **PT Reservada**, não poderá ser enviada para uma impressora de rede sem que alguém autorizado salvaguarde a confidencialidade durante a impressão e recolha do documento.[8]

---

[8] Este ponto encontra-se alinhado com a *Ordem de Serviço 001403CE* (PT SGPS)– Matérias Classificadas PT, Preparação, Manuseamento, Arquivo e Destruição. Entrada em vigor em de 01.08.2003, a sua alteração apenas é viável após revisão dessa OS.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.8 Exchange of Information

5.5.4 Utilização de Computadores Portáteis

Funcionários que utilizem computadores portáteis da PTP deverão ter um cuidado acrescido em não deixar o equipamento sem supervisão e sem o respectivo cadeado. Informação classificada apenas poderá ser guardada no respectivo portátil se estiver cifrada, não sendo suficiente a protecção de documentos por *password* usualmente disponibilizada em algumas aplicações.

Sempre que termine a colaboração de um funcionário (interno ou de uma entidade externa) a respectiva chefia deverá informar a área responsável pela Gestão de Equipamentos para que possam ser eliminados os registos de informação desse colaborador com meio adequado à confidencialidade da informação relativa à função desempenhada.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

7.1.3 Acceptable use of assets

11.7.1 Mobile computing and communications

5.5.5 Política de e-mail

Esta Política define qual a utilização apropriada de e-*mails* enviados da PTP de forma a prevenir danos na imagem da organização. É essencial que se tenha em consideração que qualquer mensagem enviada de um *domínio de e-mail* da PTP ou com assinatura contendo referência a uma entidade da PTP (neste caso mesmo que enviada de um domínio de e-mail pessoal de um colaborador) será ou poderá ser considerada pelo público em geral como uma afirmação / posicionamento oficial da organização.

Neste sentido, o *e-mail* da organização não poderá ser utilizado para a criação e distribuição de qualquer mensagem perturbadora ou ofensiva, incluindo comentários ofensivos sobre raça, género, traços físicos, deficiências, idade, orientação sexual, pornografia, convicções e práticas religiosas, orientações políticas ou naturalidades. É proibido o envio de *chain letters* de um *e-mail* da PTP.

O envio de e-mails massivos, i.e., para uma lista de distribuição de grande dimensão, apenas deverá ser efectuado por órgãos da PTP a esse tipo de comunicação alargada com os colaboradores (administração, recursos humanos, comunicação corporativa, etc.).

É aceitável que os Utilizadores PTP utilizem para fins pessoais o sistema de e-mail da organização, desde que tal uso seja devidamente moderado, não viole o código de conduta da PTP e respeite as regras estabelecidas no Regulamento Interno *supra* referido e nesta Politica.

Os Utilizadores deverão ter um cuidado adicional quando enviam *e-mail* interno da PTP para uma rede exterior. Como tal, nunca deverá ser efectuado reencaminhamento de forma automática para *e-mails* externos de qualquer e-mail interno. Informação classificada (**PT Confidencial** e **PT Reservado**) nunca deverá ser reencaminhada, a não ser que tal seja mesmo necessário e crítico para o negócio da PTP e a mensagem e respectivos anexos estejam cifrados, não devendo o código de acesso à informação ser comunicado ao destinatário na mesma mensagem que envia a informação, devendo preferencialmente tal código ser enviado através de outra plataforma/meio de comunicação.

É estritamente proibido que qualquer Utilizador envie e-mails, com meios da PTP ou dentro da PTP, sem ser através dos sistemas de e-mail autorizados. A criação de e-mails fazendo-se passar por terceiro é uma violação grave desta Política de Segurança e poderá dar origem a procedimentos disciplinares e legais.

Os Utilizadores nunca deverão abrir documentos, ficheiros, macros, ou URL's (links) que recebam em anexos de um *e-mail* cuja origem seja desconhecida ou suspeita ou de que haja suspeita de que o conteúdo possa ser prejudicial ao bom funcionamento do sistema informático. Estes *e-mails* deverão ser imediatamente apagados e posteriormente deverá esvaziar a pasta "*Itens Eliminados*". Todos os *e-mails* de *Spam*, *chain letters*, e semelhantes deverão ser imediatamente apagados (inclusive da pasta de itens eliminados) e nunca deverão ser reenviados. O Utilizador deverá igualmente reportar de imediato à entidade competente indicada no ponto 1 desta Politica qualquer suspeita que um e-mail recebido possa causar uma quebra de segurança nos sistemas da PTP, bem como qualquer suspeita de roubo de *password* ou de usurpação de identidade.

O Utilizador deverá notificar os responsáveis pela gestão operacional dos sistemas, caso a recepção de *spam* e *chain letters* se torne frequente.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

7.1.3 Acceptable use of assets

10.8 Exchange of information

5.5.6 Política de e-mail – Operação, Manutenção e Gestão

Certificados digitais deverão ser utilizados no caso de a organização ter disponível infra-estrutura de PKI. Com esta solução é possível dar garantias ao receptor que o emissor é autêntico e que a mensagem não foi alterada durante o seu percurso.

De forma a assegurar a segurança e performance dos sistemas, deverão ser realizadas regularmente tarefas de controlo de e-mails de forma aleatória e filtragens de certos ficheiros incluídos em e-mails, nomeadamente os afectados por vírus informáticos ou aqueles que pelo seu formato (e.g., `.exe`, `.bmp`) possam representar um potencial perigo para a integridade dos sistemas e tecnologias de informação e comunicações.

Por uma questão de segurança e de racionalidade económica em termos de espaço em disco e em espaço de backup, os registos e logs relativos a e-mails internos da PTP, i.e., não directamente associados a contratos com clientes, deverão ser obrigatoriamente eliminados ao fim de um período máximo de retenção determinado por Ordem de Serviço da PTP.

Os responsáveis pela gestão operacional dos sistemas e tecnologias de informação e comunicação deverão, por princípio, bloquear as portas TCP 25 em todos os sistemas (desktops, servidores, impressoras, elementos de rede, etc.) da PTP para evitar que estes possam ser usados para o envio de e-mails *"ad-hoc"* fora do controlo da infra-estrutura oficial Microsoft Exchange da PTP. Os casos em que, por razões aplicacionais e/ou de negócio, tal não seja possível deverão estar devidamente documentados como excepções à regra e deverão estar sob monitorização do SOC.

É obrigação das equipas responsáveis por esse sistema ou tecnologia de informação e comunicações, a identificação, documentação e monitorização das excepções (mais detalhe ver ponto 8).

A entidade responsável pela gestão das infra-estruturas deverá garantir que a porta 25 está fechada em todas as Estações de Trabalho (VDi's, ET's e TD's) e em todos os servidores que não tenham que usar o protocolo SMTP. As aplicações legadas que usem o protocolo SMTP e a respectiva porta 25 deverão estar cadastradas na CMDB da PTP. Todas as aplicações novas deverão, preferencialmente, usar a plataforma oficial de e-mail para emitir e-mails e sempre de forma autenticada. Em qualquer dos casos este facto deve ficar também registado na respectiva CMDB.

Finalmente, só deverão ter privilégios de administração das plataformas de e-mail da PTP (*e.g., MS Exchange*) técnicos nominalmente identificados e sujeitos à assinatura de um NDA adequado ou sujeitos a regras de confidencialidade no âmbito da relação laboral com a PTP.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

10.8.4 Electronic messaging

5.5.7 Utilização de Serviços de Messaging

É permitida a utilização de serviços de *messaging* através de:

- MS Messenger;
- Mensageiro do Sapo;
- Microsoft Office *Communicator*. ou Alcatel OTUC, conforme a solução adoptada para a ptNet.

Este canal de comunicação não poderá em qualquer circunstância ser utilizado para transmissão de informação corporativa classificada.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

7.1.3 Acceptable use of assets

10.8 Exchange of information

5.5.8 Comunicação de Informação Classificada como PT Confidencial e PT Reservada

A comunicação de informação **PT Confidencial** e **PT Reservado** para fora de um perímetro seguro da PTP deverá ser sempre feita de forma cifrada/encriptada.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.8 Exchange of information

5.5.9 Desenvolvimento de Sistemas – Utilização de Criptografia

O objectivo desta Política é proporcionar directrizes para o uso de criptografia, tendo por base a utilização de algoritmos que tenham sido revistos publicamente e sejam considerados eficazes. Deverão ser utilizados como base das tecnologias de criptografia algoritmos standard tais como AES (DES apenas se não existir alternativa válida), Blowfish, RSA, RC5 e IDEA. Estes algoritmos representam os mecanismos de cifra utilizados em qualquer aplicação aprovada.

Chaves de sistemas de criptografia simétrica deverão ter no mínimo 256 bits ou uma dimensão que assegure pelo menos o mesmo grau de segurança. Os requisitos da dimensão da chave de cifra serão revistos e actualizados de acordo com as evoluções tecnológicas.

A utilização de algoritmos de cifra proprietários não é permitida, excepto quando revisto e aprovado pela entidade responsável pela Política de Segurança da Informação.

> *ISO / IEC 17799:2000 – Information Technology – Code of practice for information security management:*
>
> *8.7.1 Information and Software Exchange Agreements*
>
> *10.3 Cryptographic Controls*

5.5.10 Comunicação de Informação entre Sistemas e Aplicações

Sempre que informação classificada tenha de circular fora de um perímetro seguro deverão ser obrigatoriamente utilizados Protocolos Seguros (*por exemplo, HTTPS, SSL/TSL, SSH ou IPSec*). De igual forma, sempre que informação classificada tenha de circular entre duas aplicações ou sistemas fora de um perímetro seguro, deverão ser obrigatoriamente utilizados Protocolos Seguros nessa comunicação. No caso de não ser possível segregar a informação classificada da informação não classificada, ter-se-á que actuar como se toda a informação fosse classificada, sendo adoptadas todas as medidas de segurança.

Nota para efeitos de RFP's e novas aquisições: *Todas as novas aplicações, sistemas e tecnologias de informação e comunicação deverão, por princípio, suportar Protocolos Seguros para comunicar entre si.*

Excepcionalmente, o protocolo FTP pode ser usado nos sistemas **legados** que tenham de transferir informação classificada e que, por razões técnicas históricas, não suportem versões seguras de transferência de ficheiros (e.g., SFTP ou SCP). Nestes casos, o acesso deverá:

- Ser apenas permitido entre os equipamentos que destes serviços necessitem, devendo o acesso estar bloqueado para todo e qualquer outro IP (e.g., através de mecanismos baseados, por exemplo, em *TCP Wrappers*). Violações a este ponto deverão constituir eventos monitorizados pelo *Security Operations Center* (SOC) da PTP;
- Ser efectuado sempre que possível através do Entreposto de Ficheiros;
- Estar cadastrado na respectiva CMDB para controlo periódico.

Os Sistemas e Tecnologias **legadas** que, por razões estritamente técnicas, não possam cumprir integralmente o disposto atrás, deverão ter devidamente documentadas na respectiva CMDB todas as suas excepções à Política. No caso de estarem no âmbito SOX, deverão adicionalmente estar sujeitos a parecer da entidade responsável pela Política de Segurança da Informação, acompanhados de uma proposta de medidas que possam, entretanto, mitigar os eventuais riscos a que estão expostos (para mais detalhe ver ponto 8.2).

Sempre que uma acção de renovação tecnológica não conduza ao cumprimento integral da "*Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações*", deverá, pelo menos, ser mantida a identificação deste sistema como uma excepção documentada, salvaguardando que nenhuma alteração possa conduzir a uma situação de risco acrescido de segurança comparativamente à situação anteriormente em produção (para mais detalhe ver ponto 8.3).

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

12.1 Security requirements of information systems

12.3 Cryptographic Controls

5.5.11 Remote Shells, SNMP e Administração de Sistemas e Tecnologias de Informação e Comunicação

Para os sistemas das e tecnologias legadas que, por razões técnicas históricas, só tenham Telnet ou outro protocolo idêntico de *remote shell* não seguro, os acessos deverão ser apenas permitidos dentro de um perímetro seguro e a partir dos IP's específicos das consolas autorizadas, devendo o acesso estar bloqueado para todo e qualquer outro IP (e.g., através de mecanismos baseados, por exemplo, em *TCP Wrappers*).

No caso de impossibilidade em identificar todos os IP autorizados (p.e: IP's atribuídos via DHCP) os acessos deverão ser efectuados via entreposto de administração[9] reconhecido pela entidade responsável pela operacionalização e gestão dos serviços de TI's.

Apenas deverão ter privilégios de administração (Sistemas, Base de Dados, Aplicações, etc.) técnicos nominalmente identificados e sujeitos à assinatura de um NDA adequado ou sujeitos a regras de confidencialidade no âmbito da relação laboral com a PTP.

Em todos os sistemas da família UNIX deverá ser proibido o login directo a "*root*". Os administradores de sistemas ou responsáveis pela operação deverão fazer primeiro login em conta própria nominal, que tenha apenas os privilégios estritamente necessários para a sua função, e sempre que necessário e só nessas circunstâncias fazer SUDO a root a partir da sua conta nominal.

Acessos SNMP são estritamente proibidos a entidades não autorizadas! Acessos SNMP não seguros (e.g., com SNMP 1.x), fora do perímetro seguro dos sistemas alvo, são proibidos.

Todos os sistemas e tecnologias novas deverão suportar SSH para acessos interactivos ao sistema, mesmo dentro de um perímetro seguro. Trata-se de uma 1ª linha de defesa

[9] Vulgarmente conhecido como "Máquina de Salto"

básica. Deverão ser evitados acessos utilizando protocolos não seguros, como por ex. Telnet.

Nota para efeitos de RFP's:

a) *Todos os novos sistemas e tecnologias de informação e comunicação deverão suportar Protocolos Seguros para a sua gestão remota (e.g., SSH).*

b) *Todos os novos sistemas e tecnologias de informação e comunicação deverão suportar a versão 3.x do SNMP.*

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

12.1 Security requirements of information systems

12.3 Cryptographic Controls

5.5.12 Garantia de Segurança nos Front-Ends Extranet/Internet

Para as soluções Internet/Extranet da PTP deverá ser obrigatoriamente utilizado o protocolo **https** nas zonas da aplicação envolvendo informação classificada podendo ser usado o protocolo **http** apenas nas situações em que toda a informação seja de carácter público. Para as soluções Intranet da PTP deverá ser obrigatoriamente utilizado o protocolo **https** nas zonas da aplicação envolvendo informação classificada podendo ser usado o protocolo **http** nas outras situações.

Em qualquer das circunstâncias, os front-ends Web das soluções atrás referidas deverão estar sempre protegidos num Datacenter da PTP dentro de uma DMZ segura, com interfaces internas (*da DMZ para os backends*) e externas (*da DMZ para a rede onde estão os Utilizadores*) devidamente protegidas e monitorizadas pelo Security Operations Center (SOC) da PTP. As DMZ's expostas à Internet deverão estar segregadas das DMZ's expostas às redes internas da PTP. Idem para as DMZ's expostas a qualquer extranet.

Se a solução for crítica para a PTP dever-se-á garantir adicionalmente múltiplos front-ends Web distintos (no mínimo 2), em "*cluster*", divididos por infra-estruturas físicas diferentes, e devidamente balanceados por um "*load balancer*" com capacidade adequada.

Desta forma assegura-se:

- Uma melhor gestão dos recursos, especialmente se a carga crescer pois facilmente se adiciona um novo servidor Web ao cluster;
- Uma menor exposição de portos IP à Extranet ou Internet, permitindo consolidar os acessos vindos do exterior e facilitar a monitorização dos mesmos pelo Security Operations Center (SOC) da PTP;
- Uma maior simplificação na configuração e gestão dos dispositivos de segurança da DMZ monitorizados pelo SOC da PTP;
- Prevenção e mitigação de eventuais ataques DoS (Denial of Service) à entrada do *load balancer*, poupando os servidores a ele conectados;

- Implementação de endereçamento virtual de serviços na rede de servidores afecta, e impedindo dessa forma que seja conhecido e acedido directamente do exterior.

Quaisquer excepções a estas regras deverão ser documentadas e justificadas, bem como comunicadas, sempre que possível previamente ou, caso tal não seja possível imediatamente após a sua verificação, à entidade responsável pela segurança, a qual emitirá parecer a este respeito.

ISO / IEC 17799:2000 – Information Technology – Code of practice for information security management:

8.7.1 Information and Software Exchange Agreements

6 Gestão de Acessos

6.1 Gestão de Acessos de Utilizadores

A PTP deve adoptar transversalmente um sistema de gestão de identidades centralizado. Nesse sistema devem estar armazenados os dados que identificam todos os Utilizadores, sem excepção, internos e externos, definindo os seus privilégios de acesso aos diferentes sistemas, tecnologias e aplicações e o período de validade de cada um desses privilégios. Por outro lado, todos os sistemas, tecnologias e aplicações devem permitir autenticar e validar os privilégios de acesso de cada um dos seus Utilizadores. As configurações de segurança de todos os sistemas, tecnologias e aplicações deverão ser adaptadas a este mecanismo.

De forma a garantir um nível de segurança adequado à organização, as seguintes regras deverão ser implementadas:

- Todos os sistemas/tecnologias/aplicações deverão ter sistemas de controlo de acessos por mecanismos de autenticação dos Utilizadores;
- Acessos a sistemas/tecnologias/aplicações devem ser conseguidos via autenticação por *user/password* que devem ser únicas para cada Utilizador individual. Não é permitida a partilha de autenticação por grupos de Utilizadores. Em casos onde, por razões técnicas ou por razões de negócio, seja necessário manter contas genéricas, será obrigatório obter a aprovação da excepção por parte da entidade responsável pela Política de Segurança e implementar mecanismos alternativos de controlo que permitam a todo o momento determinar a identidade do Utilizador. Contudo, os acessos à rede terão de ser sempre nominais!
- Sempre que possível, a interface apresentada para autenticação deverá incluir o seguinte alerta – "***Este sistema apenas deverá ser usado por Utilizadores autorizados. Ao continuar a usar este sistema o Utilizador reconhece que é um Utilizador autorizado. O Utilizador reconhece que as utilizações deste sistema são registadas e compreende que as violações à "Política de Segurança da***

Informação da PT Portugal a nível dos Sistemas e Tecnologias de Informação e Comunicações" poderão despoletar acções disciplinares bem como procedimento legal civil ou criminal."

- É proibido qualquer acesso anónimo aos sistemas ou aplicações da PTP (exemplo, *através de Utilizadores Guest*). Estas contas devem estar todas desactivadas!
- Pedidos de novos Utilizadores ou de alteração de privilégios deverão passar por um processo de validação que inclua a área de Recurso Humanos e devem ser efectuados por escrito, utilizando *templates* pré-definidos ou aplicações informáticas específicas para o efeito (exemplo, através da criação de um *ticket* para a equipa de suporte, ou via Pulso Acessos[10]) e aprovados pela respectiva chefia antes de implementados; De forma a assegurarmos o registo histórico destes processos, os registos existentes deverão ser mantidos durante um período mínimo de 2 anos.
- Privilégios atribuídos a Utilizadores externos à organização deverão expirar automaticamente no máximo ao fim de 90 dias; Excepções a esta regra poderão ser implementadas, desde que sejam identificadas pelo respectivo interlocutor autorizado da PTP, que definirá o prazo adequado para o respectivo acesso. Sempre que seja necessário prolongar este período deverá ser autorizado novo pedido, pela mesma entidade;
- Todos os *user-ids* inactivos durante 60 dias (máximo) deverão ser automaticamente bloqueados; *user-ids* inactivos durante 1 ano (máximo) deverão, se possível tecnicamente e sem impacto na rastreabilidade dos Utilizadores, ser automaticamente removidos, caso contrário deverão ser mantidos bloqueados;
- Sempre que exista uma alteração significativa de responsabilidades ou funções de um Utilizador a respectiva chefia deverá informar a área responsável pela Gestão de Utilizadores para que possam ser alterados os respectivos privilégios do Utilizador.
- Sempre que termine a colaboração de um funcionário PTP, a área de recursos humanos deverá informar as áreas responsáveis pela Gestão de Utilizadores para que esse colaborador possa ser, o mais rapidamente possível, desactivado e os seus acessos cancelados em todas as redes, sistemas de informação, plataformas tecnológicas, e pontos de acesso físico aos edifícios PT. A área de gestão de recursos humanos deverá também garantir a recolha do cartão de empregado assim como a eliminação de toda a informação de carácter biométrico associado a esse funcionário. Caso o funcionário tenha um nível hierárquico com responsabilidades de gestão ou tenha, dentro das suas funções, lidado com informação confidencial, toda a informação no seu Desktop e/ou Notebook deverá ser destruída antes que este seja reaproveitado para outro utilizador.

[10] http://acessos.pulso.telecom.pt

- Sempre que termine a colaboração de um funcionário de uma entidade externa, a área na qual desenvolveu a sua actividade deverá informar as áreas responsáveis pela Gestão de Utilizadores para que possa ser, o mais rapidamente possível, desactivado e os seus acessos cancelados em todas as redes, sistemas de informação, plataformas tecnológicas, e pontos de acesso físico aos edifícios PTP. A área interna responsável pelo serviço prestado pela entidade externa, deverá também assegurar a recolha de eventuais cartões de acesso assim como a eliminação de toda a informação de carácter biométrico associado a esse funcionário externo. Caso esse funcionário externo tenha, dentro das suas funções, lidado com informação confidencial, toda a informação no seu Desktop e/ou Notebook deverá ser destruída antes que este seja reaproveitado para outro utilizador.
- Em circunstância alguma dever-se-ão permitir Desktops ou Notebooks ligados à rede interna sem que estes tenham Utilizadores autorizados.
- Para sistemas e aplicações críticas, como, por exemplo, as relevantes no âmbito SOX, é imperativa a execução de um procedimento que reavalie a necessidade da manutenção do acesso aos Utilizadores, por parte da sua chefia, o procedimento deverá ser executado periodicamente, no mínimo anualmente.
- Nos casos de esquecimento da *password* de uma conta de acesso à rede (*Active Directory*) por parte de um Utilizador, deverá ser solicitado ao próprio ou ao interlocutor/ chefia, pela linha de suporte, informação que o identifique inequivocamente (p.e., Nome completo, Número de Contribuinte, Número de Cartão do Cidadão/ BI, morada de residência, Número de empregado, etc, não podendo esta informação estar disponível para consulta pública). Caso esta informação não seja prestada correctamente, deverá ser um interlocutor/ chefia autorizado a contactar a linha de suporte.
- Sempre que um técnico com acessos activos a contas de administração de qualquer equipamento ou cesse funções é obrigatória a suspensão imediata de todas as suas contas nesses sistemas ou equipamentos. Adicionalmente, é obrigatória a execução de um procedimento que reavalie periodicamente a necessidade da manutenção de contas com privilégios de administração em todas as tecnologias, sistemas e aplicações, quer sejam de informação (BSS ou OSS) ou de comunicação. Este procedimento deverá ser executado periodicamente, no mínimo trimestralmente
- Finalmente, todos os indivíduos com acesso a contas de administração de sistemas/tecnologias/aplicações deverão estar cobertos por NDA apropriado ou cobertos por disposição contratual ou legalmente equivalente.
- A concessão de acessos deve respeitar o princípio "*need to know*", ou seja, os acessos devem ser facultados com base nas necessidades funcionais de cada colaborador.
- Sempre que possível a concessão de acessos deve assegurar a segregação de funções dos utilizadores de desenvolvimento, teste e produção (os utilizadores

da equipa de desenvolvimento não deverão ter privilégios de acesso com permissões de escrita ao ambiente de produção);

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

6.2 Política de *Passwords* de Utilizadores (Indivíduos)

Todos os Utilizadores devem ter a sua própria *password* de acesso aos sistemas informáticos da PTP, sendo esta password pessoal e intransmissível. As *passwords* são utilizadas para as mais diversas finalidades na PTP. Algumas dessas finalidades incluem: contas de acesso a aplicações, contas de administração de sistemas, contas de plataformas de serviço, contas de administração de equipamentos de rede, contas *web*, contas de *e-mail*, protecções *screen saver*, protecções do *voice mail*, etc. Nesse sentido deverão ser implementadas as seguintes regras:

1. Após a instalação de qualquer aplicação/sistema/tecnologia na PTP dever-se-á garantir que de imediato todas as passwords de fábrica (atribuídas por defeito pelos fornecedores) de contas com privilégios de administração são alteradas de acordo com as regras definidas nesta Política de Segurança; De igual forma todas as contas de "*Guest*" ou outras não necessárias ao funcionamento da PTP deverão ser imediatamente inibidas;

2. As *passwords* atribuídas por defeito a novos Utilizadores de aplicações/ sistemas/tecnologias deverão cumprir as regras de robustez definidas nesta Política e ser obrigatoriamente alteradas após o primeiro logon. A validade dos novos Utilizadores é de 48 horas, período após o qual a conta deverá ficar bloqueada;
3. De forma a prevenir possíveis ataques à segurança da informação, o número de tentativas consecutivas de um Utilizador para autenticação num sistema/aplicação/ tecnologia deverá ser de no máximo 3 (três). Sempre que o sistema suportar, 3 tentativas falhadas de autenticação a partir do mesmo ponto, o sistema deverá bloquear o acesso a esse Utilizador a partir do ponto identificado até que um administrador reinicie a respectiva *password* (*password reset*) e impedir o processo de autenticação por um período nunca inferior a 10 minutos;
4. Sempre que a segurança de um sistema/ aplicação/ tecnologia tenha sido comprometida ou exista uma suspeita nesse sentido, o responsável do mesmo sistema/ aplicação/ tecnologia deverá:
   - Reiniciar todas as *passwords* relevantes;
   - Forçar que todas as *passwords* relacionadas com o mesmo sejam alteradas na próxima vez que cada Utilizador se autentique;

- Caso não seja possível implementar a recomendação anterior, por limitações técnicas, então o responsável deverá divulgar uma mensagem que notifique todos os Utilizadores e os informe que deverão alterar imediatamente as respectivas *passwords*;

5. Sempre que exista uma suspeita fundada que uma determinada *password* foi revelada para além do seu Utilizador, deverá proceder-se imediatamente à sua substituição, quer pelo próprio Utilizador ou pelo administrador responsável de sistema/ aplicação/ tecnologia;
6. É proibida a apresentação por uma aplicação/sistema/ tecnologia de qualquer *password* no ecrã ou impressa em papel, devendo sempre ser dissimulada durante a sua inserção;
7. Sempre que as aplicações/sistemas/ tecnologias o permitam, a *password* inicial atribuída a um Utilizador deverá ser válida apenas durante a primeira autenticação do Utilizador. Durante esse acesso, o Utilizador deverá ser forçado a alterar essa primeira *password*; Este mesmo processo também deverá ser aplicado sempre que um Utilizador se esqueça da sua *password* e esta tenha de ser reiniciada pela equipa de suporte/manutenção (*password resetting*);
8. Deverão ser implementados mecanismos automáticos em sistemas/aplicações/ tecnologias que forcem o Utilizador a periodicamente alterar a *password* de acordo com as seguintes regras:
   - No máximo uma *password* só poderá ser utilizada durante 90 dias, após o que deverá expirar e forçar a sua alteração;
   - Não deverá ser possível utilizar nenhuma das últimas 10 *passwords* usadas anteriormente;
   - Após a definição da nova *password*, o Utilizador só a poderá novamente alterar após pelo menos 1 hora;
   - Os sistemas/aplicações/tecnologias apenas deverão permitir *passwords* que estejam de acordo com as regras de construção definidas no ponto 6.4 ou 6.5;

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

6.3 Política de User-Id's e Passwords para Uso Aplicacional

Sempre que um sistema, aplicação ou base de dados *"target"* permitir o acesso directo a outros sistemas ou aplicações *"clientes"*, através de um logon sobre um *user-id* e *password*, o sistema/aplicação *"target"* deverá garantir:

1. *User-id's* distintos, e *passwords* igualmente distintas, para cada sistema ou aplicação que sejam seus "*clientes*", independentemente do método de acesso usado.

2. As *passwords* usadas deverão seguir as directrizes de construção de passwords robustas desta Política de Segurança da Informação (ponto 6.5).

3. O sistema/aplicação/base de dados "*target*" deverá, no mínimo, recusar o logon se o IP origem não pertencer a um range reconhecido.

4. De forma a prevenir possíveis ataques à segurança da informação, o número de tentativas consecutivas de um sistema/processo para autenticação num outro sistema/aplicação/ tecnologia deverá ser de no máximo 1 (uma).

5. Quando um logon falhar quer pela *password* estar errada quer pelo IP não pertencer ao range esperado o logon deverá falhar sem devolver qualquer feedback à entidade "*cliente*".

6. Todos os logons devem ser registados em *log* apropriado, mantido em zona segura, quer os *logons* tenham tido sucesso quer não.

Caso se verifiquem todos os pontos anteriores, sem excepção, e tanto as aplicações/processos "*cliente*" e o sistema/aplicação ou base de dados "*target*" residam em zonas seguras dentro de Data Centers PTP, as passwords não terão de ser alteradas de forma periódica obrigatória.

Caso contrário, os responsáveis pelo sistema ou processo "*cliente*" deverão assumir um período de expiração da password de, no máximo, um ano e garantir um processo de actualização fiável seguindo as recomendações referidas no ponto6.5 para passwords robustas.

Em qualquer dos casos, sempre que exista uma suspeita fundada que uma determinada *password* foi revelada para além da equipa responsável pela exploração dos sistemas ou tecnologias envolvidas, deverá proceder-se imediatamente à sua substituição pelo administrador responsável de sistema/ aplicação/ tecnologia;

Todas as contas aplicacionais deverão ter um responsável nominal pelos mesmos (não uma entidade, email de suporte ou sigla de departamento), devidamente

registado na plataforma centralizada de gestão de identidades (*Identity Management da PTP)*.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

6.4 Directrizes para Construção de Passwords para Utilizadores Normais (Internos ou Externos)

Todos os Utilizadores deverão estar consciencializados para a importância da escolha de uma *password* que não seja uma *password* fraca. Passwords fracas põem em risco a segurança da informação na PT Portugal pelo que são proibidas por esta Política de Segurança da Informação.

Uma *password* **fraca** é uma password com pelo menos uma das seguintes características:

- Tem menos de 8 caracteres;
- Corresponde a uma palavra que faz parte de um dicionário;
- É uma palavra de uso comum, por exemplo:
    - Nomes de família, animais, amigos, colegas, personagens de ficção, etc;
    - Termos de informática, comandos, sites, organizações, hardware ou software;
    - As palavras PT, ou qualquer outra organização do grupo PT;
    - Aniversários ou qualquer outra informação pessoal, tal como morada ou números de telefone;
    - Padrões de letras ou algarismo, por exemplo aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Qualquer uma das expressões referidas anteriormente, mas escritas do fim para o início.
    - Qualquer uma das expressões referidas anteriormente, mas precedidas ou seguidas de um dígito (exemplo, PT1, 1PT) ou de um conjunto sequencial de dígitos (ex. PT123, 123PT).

Assim, as *passwords* de Utilizadores normais na PTP não deverão ser passwords fracas e deverão garantir as seguintes características[11]:

- Têm pelo menos 8 caracteres;
- Contêm letras minúsculas e maiúsculas (exemplo, a-z, A-Z)

---

[11] Para verificar se uma *password* é considerada adequada para contas normais (i.e., que não sejam de administração ou de integração aplicacional) pode recorrer ao seguinte serviço de testes da robustez de passwords disponibilizado pelo Portal Pulso: http://pwd-tester.pulso.telecom.pt. Este teste é feito localmente no próprio Browser do utilizador sem que qualquer informação seja transferida pela rede ou para o Pulso.

- Têm dígitos e caracteres de pontuação para além de letras (exemplo, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Não são uma palavra em qualquer língua, dialecto ou calão;
- Não são baseadas em informação pessoal;
- Não contêm o *username* do respectivo Utilizador;

Finalmente, as *passwords* nunca devem ser escritas ou registadas no computador. Os funcionários deverão criar *passwords* que consigam facilmente memorizar.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

11.3 User responsibilities

6.5 Directrizes para Construção de Passwords Robustas para Utilizadores com Privilégios de Administração e para Integração Aplicacional

As *passwords* de Utilizadores com privilégios de administração, e para integração aplicacional, devem ser **robustas** de acordo com as seguintes características[12]:

- Têm pelo menos 12 caracteres;
- Contêm letras minúsculas e maiúsculas (exemplo, a-z, A-Z)
- Têm dígitos e caracteres de pontuação para além de letras (exemplo, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./), que deverão estar incluídos e intercalados no interior da *password* .
- Não contêm palavras em qualquer língua, dialecto ou calão;
- Não são baseadas em informação pessoal;
- Não contêm o user name do respectivo Utilizador;

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

11.3 User responsibilities

[12] Para verificar se uma *password* é considerada adequadamente forte pode recorrer ao seguinte serviço do Portal Pulso: https://pwd-tester.pulso.telecom.pt. Este teste é feito localmente no próprio Browser do utilizador sem que qualquer informação seja transferida para o Pulso.

6.6 Responsabilidades Específicas dos Utilizadores

6.6.1 Segurança das Estações de Trabalho (ET) (VDi's, Desktops e Notebooks)

É proibido aos Utilizadores:

(a) Efectuar acções que possam danificar, interromper ou gerar erros nos sistemas informáticos da PTP;

(b) Efectuar uploads, downloads ou transmissão não autorizada de qualquer programa ou ficheiro sobre o qual incidam direitos de autor, direitos conexos ou outros direitos de propriedade intelectual, nomeadamente ficheiros de música, vídeos, etc., para fins não profissionais;

(c) Proceder à instalação de *cookies*.

Todas as estações de trabalho, independentemente de serem VDi's, Desktops ou Notebooks, devem ser instaladas pela estrutura da PTP responsável pela gestão de desktops, e devem garantir suporte activo ao conjunto de mecanismos de protecção estipulados pelas regras de segurança em vigor na PTP: *Antivírus*, *Anti-Spam*, *Anti-Spyware*, *Anti-malware*, *Personal Firewall, Screen-saver activo com password*, etc.. Estes mecanismos devem estar sempre activos e devem ser automaticamente actualizados. Os Utilizadores não podem alterar estas configurações nas suas estações de trabalho de forma a garantir a segurança da informação no uso da mesma. Excepções a esta regra deverão ser previamente autorizadas pela entidade responsável pelas estações de trabalho.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

11.3 User responsibilities

6.6.2 Segurança das Estações de Desenvolvimento (TD) (Desktops ou Notebooks)

Todas as estações de trabalho devem ser instaladas pela estrutura da PTP responsável pela gestão de desktops, e devem garantir suporte activo ao conjunto de mecanismos de protecção estipulados pelas regras de segurança em vigor na PTP: *Antivírus*, *Anti-Spam*, *Anti-Spyware*, *Anti-malware*, *Personal Firewall, Screen-saver activo com password*, etc. Estes mecanismos devem estar sempre activos e devem ser automaticamente actualizados. A alteração destas configurações, bem como a instalação/ desinstalação de software ,é da responsabilidade do respectivo Utilizador a quem a estação de desenvolvimento foi atribuída.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

11.3 User responsibilities

6.6.3 *Lock* e *Logout* do seu Computador

Utilizadores que deixem o seu posto de trabalho sem supervisão durante algum tempo deverão previamente garantir que efectuam o *Lock* ou *Logout* do seu computador.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.3 User responsibilities

6.6.4 Escolha de *Passwords*

As *passwords* escolhidas deverão ser robustas de acordo com as directrizes de construção de *passwords* descritas no ponto 6.4.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.2. User access management

11.3 User responsibilities

6.6.5 Protecção das *Passwords*

Os Utilizadores não deverão utilizar a mesma *password* para acessos na PTP e para acessos externos à PTP (exemplo, acesso a um *ISP*, acesso à banca *on line*, etc.). As *passwords* nunca deverão ser partilhadas com ninguém, incluindo assistentes administrativos ou secretárias. **Todas as *passwords* deverão ser tratadas como informação classificada da organização**.

Eis uma lista do que **NÃO** deverá ser feito pelos funcionários:

- **Não** deverão revelar a sua *password* por telefone a ninguém;
- **Não** deverão revelar a sua *password* em nenhuma mensagem de *e-mail*;
- **Não** deverão revelar a sua *password* à sua chefia;
- **Não** deverão falar de uma *password* na presença de outras pessoas;
- **Não** deverão revelar pistas sobre a sua *password* (exemplo, "*o meu nome de família*");
- **Não** deverão revelar a sua *password* em inquéritos ou outros meios;
- **Não** deverão partilhar a sua *password* com membros da família;
- **Não** deverão revelar a sua *password* a colegas quando vai de férias;
- **Não** deverão revelar utilizar a funcionalidade *"Remember Password"* disponível em algumas aplicações (exemplo, OutLook, Netscape Messenger);
- **Não** deverão escrever a sua *password* e guardá-la no escritório ou em qualquer dispositivo, incluindo o seu computador, telemóveis, PDA's ou Smart Phones;

Se alguém pedir a indicação de uma *password*, os funcionários não a deverão disponibilizar e deverão relembrar a essa pessoa a presente Política.

As *passwords* deverão ser alteradas, no mínimo, trimestralmente.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *11.2. User access management*
>
> *11.3 User responsibilities*

6.6.6 Partilha de Informação

A partilha de discos com privilégios de leitura/escrita deverá ser evitada. Para a partilha de informação deverão ser utilizados os sistemas existentes na organização (exemplo, *Shares*, *Intranets, etc*) para as quais se encontram definidas e implementadas as necessárias políticas de acesso.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *11.2. User access management*
>
> *11.3 User responsibilities*

6.6.7 Comunicação de Situações Anómalas

Sempre que um Utilizador suspeite de um uso indevido de uma sua conta de acesso a um sistema/ aplicação/ tecnologia, ou que a sua *password* tenha sido revelada, deverá informar imediatamente o SOC de acordo com o descrito na secção 8.4desta Política – Comunicação de Incidentes de Segurança.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *13.1 Reporting information security events and weaknesses*

6.6.8 Destruição, Alteração ou Comprometimento não Autorizado de "*Logs*" Aplicacionais ou de Sistema

Os Utilizadores não podem destruir, alterar ou comprometer quaisquer "*logs*" aplicacionais ou de sistema. O não cumprimento desta regra constitui uma violação grave a esta Política. Excepções a esta regra deverão ser devidamente justificadas e aprovadas pela entidade responsável pela Política de Segurança da Informação.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *11.3 User Responsibilities*
>
> *13.1.2 Reporting security weaknesses*

6.6.9 Realização de Testes Não Autorizados de Segurança

Os programas de testes e demonstração que não pertençam à PTP só poderão ser utilizados após exame e autorização prévia por da entidade responsável pela Segurança da Informação referida no ponto 1, designadamente no que respeita a vírus e/ou compatibilidade.

Os Utilizadores não poderão, em caso algum, executar operações informáticas que possam constituir violação de quaisquer disposições legais aplicáveis.

Os Utilizadores não podem testar ou comprometer as medidas de segurança associadas aos sistemas. Incidentes envolvendo captura e análise de tráfego (*network tapping* ou *sniffing*), tentativa de acesso não autorizado a sistemas, aplicações ou plataformas de comunicações, *password cracking*, decifração de ficheiros de terceiros, ou outras actividades similares geralmente classificadas como "*hacking*", que podem comprometer a segurança dos sistemas e tecnologias de informação e comunicação, serão consideradas violações graves desta Política. Excepções a esta regra deverão ser devidamente justificadas e aprovadas pelas chefias correspondentes, e comunicadas à entidade responsável pela Política de Segurança da Informação.

6.6.10 Outras Disposições

A PTP disponibiliza aos seus colaboradores programas anti-vírus, cuja utilização e resultados não vinculam, sob qualquer forma, a PTP. O facto de o programa examinar as disquetes, CDs, DVDs ou dispositivos de armazenamento de informação (ex. USB pens) do Utilizador nos computadores da PTP não implica a autorização para a sua utilização.

Uma vez que os Recursos Informáticos e de Comunicação são disponibilizados pela PTP como instrumentos de trabalho auxiliares ao desempenho da actividade contratada, constituindo a possibilidade da sua utilização para fins privados uma mera liberalidade da empresa, esta reserva o direito de, sem prejuízo da manutenção da vigência da presente Política, revogar a todo o tempo e sem qualquer aviso prévio, a utilização dos recursos informáticos e de comunicação para fins profissionais com a inerente obrigação do Utilizador entregar imediatamente todos os recursos informáticos e de comunicação que se encontrem em seu poder.

6.6.11 Obrigações no Momento de Cessação de Vínculo Laboral ou Contratual

Em caso de cessação do contrato de trabalho, seja por que razão for (incluindo assim despedimento, reforma e situações análogas) ou mudança de funções, o Utilizador é obrigado a:

a) entregar ao seu superior hierárquico os equipamentos, software e demais ferramentas de trabalho e informação elaborada e/ou em seu poder, não podendo

conservar ou utilizar qualquer da referida informação para qualquer efeito, sem autorização prévia e escrita da PTP;

b) eliminar todas as mensagens e informação de natureza pessoal que tenha armazenado ou que se encontrem disponíveis nos sistemas da empresa e/ou nos recursos electrónicos disponibilizados pela mesma;
c) entregar os e-mails de carácter profissional ao seu imediato superior hierárquico, em formato digital.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.3 User Responsibilities

13.1.2 Reporting security weaknesses

6.7 Controlo de Acessos à Rede

6.7.1 Utilização de Linhas Analógicas, ISDN e ADSL

A utilização de *kits ADSL* ou *Modems* (analógicos ou ISDN) para ligação de desktops ou notebooks simultaneamente à *Internet* e a qualquer das redes internas da PTP (incluindo redes de gestão) é expressamente proibida. Excepções a esta regra deverão ser devidamente justificadas e aprovadas pelas chefias correspondentes, e comunicadas à entidade responsável pela operacionalização e gestão dos serviços de TI's, incluindo a sua segurança operacional. Enquanto um desktop ou notebook estiver ligado a uma das redes internas da PT não pode estar ligado a qualquer outra rede. Só pode haver uma ligação de cada vez.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

6.7.2 Utilização de Redes *Wireless*

As organizações da PTP que, por necessidades operacionais, tenham que disponibilizar acessos *Wireless* (WiFi, 3G, etc.) aos seus Utilizadores, deverão assegurar autorização prévia à área responsável pela segurança operacional das redes internas da PTP. Essa entidade deverá verificar a segurança desta rede *Wireless* e do acesso desta às redes internas da PTP. Caso não seja possível garantir a segurança da informação dos Utilizadores nessa rede e/ou a segurança do acesso a redes internas da PTP, a rede Wireless não deverá ser autorizada.

Acessos dentro de instalações PTP, com ET's ou TD's PTP, a redes *Wireless* não autorizadas serão considerados violações graves a esta Política.

Igualmente deverá ser considerada violação grave, toda e qualquer instalação de equipamentos *Wireless* (exemplo, *routers* com interface WiFi) não autorizados e que

disponibilizem a outros equipamentos (exemplo, *laptops* ou computadores pessoais) acesso directo à rede interna da PTP.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

6.7.3 Túneis para o Exterior

A abertura de túneis que permitam a comunicação de dados a partir da rede interna da PTP para o exterior, sem ser devidamente analisada, documentada e autorizada pelas chefias correspondentes e pela entidade responsável pela Política de Segurança da Informação, é expressamente proibida (para mais detalhe ver glossário).

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

6.7.4 Acessos Remotos

Os acessos remotos para o interior da empresa deverão recorrer sempre, sem excepção, a VPN's oficiais geridas pela entidade responsável pela Infra-estruturas. A segurança operacional destas VPN's deverá ser igualmente da responsabilidade operacional daquela entidade.

Os pedidos de acesso a partir do exterior deverão ser devidamente analisados, documentados e autorizados pelas chefias. A organização deverá ter definido um procedimento de suporte aos pedidos de acesso remoto e respectivas autorizações, devendo existir informação consolidada sobre quem tem este tipo de acesso (quem tem acesso? quem autorizou? qual a infra-estrutura utilizada? perfil do acesso).

Deverá ser mantido um registo dos acessos efectuados, assegurando um histórico mínimo de 2 anos.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

6.7.5 Acessos a Extranet(s)

Todos os pedidos de novas ligações a uma *extranet* deverão ser formalizados por escrito pela entidade requisitante junto da equipa responsável pela *extranet*, incluindo uma justificação clara do requisito de negócio subjacente. Estes pedidos deverão ser enviados pela equipa responsável pela *extranet* para a entidade responsável pela criação destes acessos de forma a serem revistos e autorizados. Esta revisão tem como objectivo assegurar que todos os acessos estão de acordo com os requisitos de negócio e as politicas de segurança definidas e que o princípio de "*acesso apenas ao que é necessário*" é cumprido.

A disponibilização de novas conexões entre terceiras partes e a PTP tem de ser formalizada através de contrato, o qual deverá estar em estrita conformidade com os termos da presente Política. Este contrato deverá ser assinado pelos representantes das respectivas organizações que detenham o poder para as representar legalmente.

A área da PTP responsável pelo pedido de conexão deverá designar um colaborador que será o ponto de contacto para tudo o que esteja relacionado com esta ligação *extranet*. Este colaborador actua em nome da área da PTP responsável pelo pedido de conexão e é responsável pelo cumprimento desta Política e do acordo estabelecido com a entidade externa. Caso seja alterado este ponto de contacto, a entidade responsável pela gestão da *extranet* deverá ser informada e deverá ser identificado um novo colaborador para assumir estas funções.

Todas as conexões estabelecidas deverão ser baseadas no princípio de "*acesso apenas ao que é necessário*", de acordo com os requisitos de negócio e a revisão efectuada pela entidade responsável pela criação dos acessos. Em nenhum caso deverá a PTP depender da entidade terceira para a protecção da sua rede e recursos.

As alterações a um acesso já existente deverão ser requeridas seguindo o mesmo processo de um novo pedido, descrito anteriormente.

Quando um acesso já não é necessário, a entidade requerente, através do colaborador identificado como ponto de contacto (colaborador que deverá desempenhar funções de contacto com a equipa responsável pela Extranet, no que se refere à respectiva ligação, bem como assegurar o cumprimento desta Política por parte dos Utilizadores e equipas da Extranet), deverá notificar a equipa responsável pela *extranet*, que irá desactivar esse acesso à *extranet*. Esta acção poderá corresponder a uma modificação das permissões existentes (exemplo, remoção de um *Utilizador*) ou à desactivação total da conexão daquela entidade terceira. Este processo deverá ser revalidado no mínimo semestralmente, de forma a garantir que as conexões existentes ainda são necessárias.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

6.8 Controlo de Acessos a Sistema Operativo

6.8.1 Directrizes de Configuração de Estações de Trabalho (ET e TD)

As Estações de Trabalho de todos os colaboradores devem ter um Antivírus, *Anti-Spyware* e *Personal Firewall* activos e com actualizações automáticas. O Utilizador da Estação de Trabalho (TD) deve ser impedido de alterar a configuração destes programas. No caso de Estações de Trabalho virtuais (VDi's) sem qualquer possibilidade de ler ou escrever dados e/ou programas a partir de drives USB, *Disquette*, CD/DVD ou outros,

mecanismos de protecção equivalentes poderão ser implementados ao nível da plataforma de virtualização e não necessariamente ao nível de cada "*Desktop Virtual*".

O *screen saver* deverá estar configurado para, após cinco minutos de inactividade no posto de trabalho, o mesmo ser activado protegendo o acesso por *password*.

Na altura da autenticação dos Utilizadores que pretendem utilizar um posto de trabalho, os servidores de domínio devem validar e forçar a configuração de segurança acima referida. Caso o posto de trabalho não cumpra com algum dos critérios a sua entrada na rede deve ser recusada.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

11.4 Network access control

11.5 Operating system access control

6.8.2 Directrizes de Configuração de Estações de Trabalho de Risco

Qualquer Estação de Trabalho deve ser instalada de acordo com as regras de segurança em vigor na PTP, incluindo activações de *screen-saver*, *anti-spyware* e *personal firewall*, bem como actualizações automáticas, estando os Utilizadores proibidos de alterar as respectivas configurações, salvo com prévia autorização da entidade responsável pela aplicação em causa.

Entende-se como Estação de Trabalho de risco as que se encontram mais expostas e como tal apresentando maior risco de utilização por Utilizadores não autorizados, como por exemplo as lojas e *call centers* da PTP.

Deverá existir uma estação padrão com acesso e privilégios de utilização mais restritivos para as situações em que sejam consideradas Estações de Trabalho de risco.

Qualquer Utilizador que se autentique numa destas Estações de Trabalho terá apenas acesso à funcionalidade e aplicações definidas para o perfil deste posto de trabalho. Apenas existirá uma excepção a esta regra para os colaboradores da equipa de suporte/manutenção.

Estas estações padrão deverão conter software antivírus, *anti-spyware* e *firewall* activados de modo a fornecer um nível de segurança adequado à organização. O *screen saver* deve estar configurado para activar após dois minutos de inactividade no posto de trabalho, protegendo o acesso por *password*, de forma a prevenir acessos não autorizados por ausência do Utilizador (exemplo, o funcionário da loja tem que se deslocar do posto de trabalho para ir ao armazém buscar um equipamento para o cliente).

Estas Estações de Trabalho de risco não deverão ter disponíveis as drives para meios amovíveis, diminuindo assim o risco da existência de cópias não autorizadas da informação da PTP.

No caso de Estações de Trabalho virtuais (VDi's) sem qualquer possibilidade de ler ou escrever dados e/ou programas a partir de drives USB, *Disquette*, CD/DVD ou outros, mecanismos de protecção equivalentes poderão ser implementados ao nível da plataforma de virtualização e não necessariamente ao nível de cada "*Desktop Virtual*".

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

11.4 Network access control

11.5 Operating system access control

6.8.3 Acesso Remoto a Equipamento

Deverão ser utilizados Protocolos Seguros, sempre que os sistemas o permitam.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.4 Network access control

11.5 Operating system access control

6.8.4 Acessos a Servidores e outras Tecnologias de Informação

Todos os servidores, sistemas de *storage* e *backup* e outras tecnologias de informação críticas para a PTP deverão estar sob a responsabilidade de um grupo operacional que assegure a sua administração, operacionalidade e segurança. Os servidores deverão estar sempre localizados num ambiente em que exista um rigoroso controlo de acessos físicos, bem como condições ambientais adequadas para a manutenção do equipamento / sistemas.

6.8.5 Acessos a Elementos de Rede e Segurança de Rede

Todos os *routers*, *switches*, *firewalls*, *IDS's*, *IPS's* e outros elementos de redes da PTP deverão estar sob a responsabilidade de grupos operacionais que assegurem a sua administração e segurança. Estes elementos de rede deverão estar sempre localizados em ambientes em que exista um rigoroso controlo de acessos físicos, bem como condições ambientais adequadas para a sua operação e manutenção.

6.8.6 Directrizes de Configurações

- A configuração dos sistemas operativos deverá ser sempre efectuada tendo em consideração as normas de segurança emitidas pelos respectivos fornecedores e/ou elaboradas pelas áreas operacionais, bem como os normativos emitidos pela entidade responsável pela Política de Segurança da Informação.
- O acesso a serviços deve ser protegido por mecanismos de controlo de acessos, por exemplo *TCP wrappers* ou *Host Firewalls* se possível.
- Deverão ser instalados imediatamente os *patches* de segurança assim que emitidos, sendo a única excepção quando se verificar que a sua aplicação imediata interfere com um requisito de negócio.
- As relações de confiança entre sistemas são um risco de segurança, devendo ser evitado o seu uso. Esta solução só poderá ser utilizada se não existir nenhuma opção de comunicação alternativa.
- Os privilégios de acesso devem ser definidos tendo por base o princípio que cada Utilizador só pode executar as acções estritamente necessárias na sua função.
- Sempre que exista disponível um canal de comunicação seguro (se for tecnicamente exequível), acessos privilegiados deverão ser efectuados sobre estes canais (exemplo, conexões cifradas utilizando, por exemplo, HTTPS, SSH, SSL/TSL, SFTP, SCP ou IPSec).

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

9.2 Equipment security

11.4 Network access control

11.5 Operating system access control

6.9 Controlo de Acessos a Aplicações

6.9.1 Standards para Desenvolvimento de Aplicações

As equipas de desenvolvimento deverão garantir que as soluções por si desenvolvidas contêm as seguintes precauções de segurança:

- As aplicações devem suportar a autenticação de Utilizadores individuais (nominalmente identificados) e não de grupos;
- Mesmo nas aplicações residentes em zonas seguras dentro de um Data Center, não devem haver *passwords* directamente escritas no meio do código aplicacional ou no meio de *scripts*. Quando não houver alternativa prática, face à base tecnológica em uso (e.g., tecnologias tecnologicamente obsoletas), dever-se-á garantir que, pelo

menos, as *passwords* residem em ficheiro próprio devidamente protegido, preferencialmente encriptado, e só acessível à aplicação ou script que dela precisa.

- Quando a componente *"cliente"* de uma aplicação, a funcionar num desktop/notebook, precisar de aceder directamente a outra aplicação secundária deverá obrigar o Utilizador a fazê-lo explicitamente ou recorrer ao processo de *Single-Sign-On* da PTP. Em caso algum deverá a *password* da aplicação secundária residir embutida no código da componente *"cliente"*, especialmente se este for interpretado.
- Devem providenciar um nível de perfis que permita suportar as diferentes funções de negócio dos Utilizadores, assegurando a segregação de funções de acordo com a matriz definida pelo controlo interno (OS 001108 CE – PT SGPS);
- Devem providenciar algum tipo de gestão de perfis, para que um Utilizador possa assumir as funções de outro sem que tenha que saber a *password* do colega, observando sempre que possível o ponto anterior;
- As aplicações que lidem com informação classificada devem ser testadas contra vulnerabilidades de segurança dentro das melhores práticas de segurança aplicacional (e.g., *buffer overflows*, *sql injection*, etc.);
- As aplicações que lidem com informação classificada devem garantir um "*audit trail*" relativo às alterações a essa informação classificada indicando, no mínimo:
    a) Operação realizada (consulta só obrigatória para informação classificada acima de Confidencial);
    b) Alteração feita (valor antigo, valor novo);
    c) Estado da operação (e.g., sucesso ou insucesso)
    d) *Timestamp* da operação;
    e) Quem realizou a operação (user-id);
    f) IP Origem;
- Esta informação deve estar disponível por um período mínimo a definir para cada uma das aplicações, devendo também ser definido, em função da finalidade e necessidade da recolha dessa informação, o período máximo de conservação da mesma, de modo a garantir o rigoroso cumprimento das leis de protecção de dados, nomeadamente no que toca à eliminação de informação contendo dados pessoais.
- Deve suportar *TACACS+*, *RADIUS*, *LDAP ou Single Sign On*, sempre que possível.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.6 Application and information access control

12.1 Security requirements of information systems

6.9.2 *Passwords* de Acesso a Bases de Dados

Esta Política estabelece os requisitos para armazenar e devolver *User Names* e *Passwords* de Base de Dados (ou seja, as credenciais de Base de Dados) a serem utilizados por uma determinada aplicação que acede a uma Base de Dados da PTP. As aplicações disponíveis na rede PTP necessitam habitualmente de aceder a um ou mais servidores de Base de Dados. De forma a ser possível aceder a uma Base de Dados, as aplicações têm que se autenticar na Bases de Dados através da apresentação das credenciais necessárias. Os privilégios de acesso às Base de Dados, cujas credenciais deverão restringir, poderão ser comprometidos se estas mesmas credenciais forem guardadas de forma incorrecta pelas aplicações.

De forma a manter a segurança das Bases de Dados da PTP, o acesso por aplicações deverá apenas ser permitido mediante a apresentação das necessárias credenciais. Estas credenciais não deverão residir no corpo do código da aplicação em texto nem deverão ser armazenadas numa localização acessível através de um *web server* e da utilização de protocolos inseguros.

6.9.2.1 Armazenamento de *User Names* e *Passwords* de acesso a Bases de Dados

- Os *User Names* e *Passwords* de acesso a Bases de Dados podem ser guardados em zona segura num ficheiro separado do código da aplicação. Este ficheiro não deverá ser num formato que permita a sua leitura.
- As credenciais de Base de Dados podem residir no servidor. Neste caso, um número de *hash* que identifique as credenciais poderá estar incluído no código da aplicação.
- As credenciais de Base de Dados podem residir num servidor de autenticação, tal como um servidor *LDAP* utilizado para autenticação de Utilizadores. A autenticação da aplicação na Base de Dados pode ocorrer como parte do processo de autenticação de Utilizador no servidor de autenticação. Neste caso, não existe necessidade de utilização de credenciais a nível da programação da aplicação.
- As credenciais de Base de Dados não podem residir na árvore de documentos de um *web server*.
- A autenticação de Utilizadores de base de dados *Oracle* nunca deve usar o mecanismo *Oracle* que delega essa tarefa no sistema operativo do cliente, também conhecido por autenticação *OPS$*.
- Para linguagens executáveis a partir do código, as respectivas credenciais não devem residir no mesmo directório onde se encontra o código-fonte.
- *As passwords* utilizadas para acesso a Base de Dados deverão estar de acordo com as directrizes de criação de *Passwords* descritas no ponto 6.5.

6.9.2.2 Extrair *User Names* e *Passwords* de Bases de Dados

- Se estiverem guardados num ficheiro, os *User Names* e *Passwords* de acesso a Bases de Dados deverão ser lidos no momento imediatamente anterior à sua utilização. Imediatamente a seguir à autenticação na Base de Dados, a memória contendo o *User Name* e *Password* deverá ser limpa ou libertada.

6.9.2.3 Acesso a *User Names* e *Passwords* de Bases de Dados

- Cada aplicação que implemente uma função de negócio deverá ter credenciais únicas de Bases de Dados. A partilha de credenciais por diversas aplicações não é permitida.
- As *Passwords* utilizadas para acesso a Bases de Dados deverão estar de acordo com as directrizes para construção de *passwords* definidas no ponto 6.5. As equipas responsáveis pelas Bases de Dados deverão ter um processo definido que garanta que as *passwords* de Bases de Dados são controladas e devendo incluir um método para restringir o conhecimento das *passwords* de Bases de Dados apenas a quem necessita.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.6 Application and information access control

12.1 Security requirements of information systems

6.9.3 *Passwords* de Acesso a Aplicações

Mesmo nas aplicações residentes em zonas seguras dentro de um Data Center, não devem haver *passwords* directamente escritas no meio do código aplicacional ou no meio de *scripts*. Quando não houver alternativa prática, face à base tecnológica em uso (e.g., tecnologias tecnologicamente obsoletas), dever-se-á garantir que, pelo menos, as *passwords* residem em ficheiro próprio devidamente protegido e encriptado e só acessível à aplicação ou script que dela precisa.

Sempre que as aplicações armazenem os identificadores dos seus Utilizadores e as respectivas *passwords* dentro de uma tabela numa base de dados deverão fazê-lo de forma cifrada, para ambas as colunas (*login e password*). A chave de cifra não deverá ser armazenada dentro da base de dados, recomendando-se a utilização de um ficheiro de configuração da aplicação com acesso protegido.

Quando a componente *"cliente"* de uma aplicação, a funcionar num desktop/notebook, precisar de aceder directamente a outra aplicação secundária, deverá obrigar o Utilizador a fazê-lo explicitamente ou recorrer ao processo de *Single-Sign-On* da PTP. Em

caso algum deverá a *password* da aplicação secundária ser embutida no código da componente *"cliente"*, especialmente se este for interpretado.

As aplicações novas que lidem com informação classificada deverão garantir autenticação via rede através de Protocolos Seguros com base criptográfica (exemplo, HTTPS, SSH, SSL/TSL, ou IPSec).

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.6 Application and information access control

12.1 Security requirements of information systems

6.10 Monitorização de Acessos

Os sistemas operativos, bases de dados e aplicações devem funcionar com o sistema de monitorização de acessos activo. No seu nível mínimo de funcionamento, este sistema deve registar entradas e saídas assim como acessos a dados classificados (**PT Confidencial**, **PT Reservado**, dados de cliente, dados de negócio ou outro tipo de dados protegidos por legislação).

Os sistemas e tecnologias mais críticas, incluindo todos os sistemas e aplicações SOX, todas as DMZ's, todos os dispositivos de segurança, e todos os sistemas e elementos de rede mais relevantes, deverão estar sob monitorização no SOC da PTP.

Deverão ser estabelecidos processos de monitoria que permitam:

- Detectar entradas ou tentativas de entradas ilegítimas nos sistemas;
- Detectar práticas que coloquem em risco as salvaguardas do controlo de acessos;
- Detectar tentativas de aumentar os privilégios atribuídos;
- Garantir a existência de provas suficientes, para melhorar os procedimentos de segurança e/ou permitir accionar procedimentos disciplinares ou processo criminal ou cível, quando algum incidente ocorrer;
- Permitir definir modelos de comportamento normais, que permitam, por comparação, detectar cenários anómalos.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.10 Monitoring

7 Disposições Adicionais ao Nível da Gestão e Administração de Sistemas, Bases de Dados e Aplicações

7.1 Garantia de Zonas Seguras (Perímetros Seguros)

Todos os sistemas e aplicações relevantes deverão estar, sempre que possível, em perímetros seguros, tanto ao nível físico como ao nível lógico. Apenas os *frontends* aplicacionais deverão ficar expostos numa DMZ.

Ao nível da **segurança física**, para um perímetro ser considerado seguro, terá de estar totalmente protegido dentro de um *Datacenter* oficial da PTP e o acesso físico ao mesmo terá de implicar a identificação, autorização, controlo e acompanhamento de quem quer que pretenda o acesso. As excepções a esta regra serão os técnicos do *Datacenter* ou as equipas de administração que normalmente trabalhem na zona onde se encontra o perímetro em causa.

Ao nível da **segurança lógica,** para um perímetro ser considerado seguro na PTP, terá de garantir que, sem excepção, **todos** os acessos por rede a qualquer dos sistemas ou tecnologias dentro ou nesse perímetro sejam previamente conhecidos e comprovadamente monitorizados e controlados por sistemas de segurança operacional da PTP (Firewalls e IDS's/IPS's) devidamente integrados no SOC da PTP. Adicionalmente, um perímetro só será considerado seguro se todos os sistemas e elementos de rede nele contidos estiverem seguros de acordo com as melhores práticas de segurança de informação e não exista qualquer relação de confiança entre um sistema dentro do perímetro seguro e um outro sistema fora desse perímetro.

Finalmente, um perímetro seguro exige obrigatoriamente que a sua administração, quando remota, recorra, sem excepção, a Protocolos Seguros e a consolas seguras.

A entidade responsável pela Política de Segurança da Informação deverá periodicamente (pelo menos uma vez por ano) e sempre que considere necessário, efectuar peritagens à segurança lógica e física dos perímetros seguros da PTP.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

11.6 Application and information access control

11.4.5 Segregation in networks

7.2 *"Hardening"* de Sistemas, Bases de Dados, Aplicações e Elementos de Rede

Deverá ser garantido que em todos os sistemas se elimine o maior número de possíveis riscos de segurança, desabilitando todas as contas, serviços, interfaces (*incluindo portas IP*) desnecessárias à sua função final. Em particular, os *frontends* aplicacionais Web expostos na *internet/extranets* deverão ser sujeitos a *security hardening*[13] de acordo com as melhores práticas existentes para a tecnologia em causa.

Os sistemas que deixem de ter funções operacionais, porque foram entretanto substituídos por sistemas mais actuais ou por qualquer outra razão, não deverão permanecer acessíveis nas redes internas da PTP. Enquanto não forem definitivamente desligados ou reaproveitados para outras funções, deverão permanecer sob controlo da segurança operacional do respectivo datacenter.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *10.4 Protection against malicious and mobile code*
>
> *11.4.4 Remote diagnostic and configuration port protection*

7.3 Acessos a *Root* e Execução de Comandos

Apenas deverão ter privilégios de administração (Sistemas, Base de Dados, Aplicações, etc.) técnicos nominalmente identificados e sujeitos à assinatura de um NDA adequado ou sujeitos a regras de confidencialidade no âmbito da relação laboral com a PTP.

Para sistemas da família UNIX não deverão ser efectuados acessos *root* remotos directamente.

Deverá ser sempre feito o acesso como Utilizador nominal e posteriormente elevar privilégios para root, garantindo que existem *audit logs* do processo.

> *ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management*
>
> *11.5 Operating System Access Control*

7.4 Aplicação de *Patches*

Deve ser garantido, pelos responsáveis de cada sistema, que todos os *patches* lançados pelo fabricante, e especialmente os *patches* relativos à segurança, estejam devidamente

---

[13] As melhores práticas são internacionais e estão bem suportadas, por exemplo, pelo NIST (www.nist.org), SANS (www.sans.org), CyLab, etc.

instalados no sistema, com a excepção de causar impacto no bom funcionamento dos sistemas.

Estas actualizações deverão ser formalmente planeadas, devendo ser identificados os riscos associados e definidos os planos de testes e os procedimentos de *fall-back*.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

10.4 Protection against malicious and mobile code

12.5.2 Technical review of applications after operating system changes

12.6 Technical Vulnerability Management

8 Excepções à Política de Segurança da Informação e Comunicação de Incidentes de Segurança

8.1 Novos Sistemas e Tecnologias

Para os novos Sistemas e Tecnologias, em que se verifiquem situações em que a Política de Segurança da Informação não seja aplicável por razões técnicas e/ ou funcionais, a equipa responsável por esse sistema ou tecnologia deverá proceder à identificação das excepções, documentar as mesmas. A documentação deverá incluir medidas que possam, entretanto, mitigar os riscos em causa. Após documentadas e registadas na CMDB respectiva ou, na falta desta, em meio equivalente, estas excepções deverão ser aprovadas pelos seguintes Directores de primeira linha:

- No caso de excepções relativas a TI's:
    - Situações da estrita responsabilidade da entidade responsável pela operacionalização e gestão dos serviços de TI's da PTP e que não tenham impacto na segurança de qualquer SI (BSS e OSS): bastará nestes casos a aprovação do Director responsável pela operacionalização e gestão dos serviços de TI's;
    - Situações mais complexas que possam também pôr em causa, directa ou indirectamente, a segurança da informação residente ou processada por SI's (BSS ou OSS): para além da aprovação do Director responsável pela operacionalização e gestão dos serviços de TI's, a excepção deverá ter adicionalmente a aprovação do Director responsável pela exploração e operação dos SI's na PTP;
- No caso de excepções relativas a SI's (BSS ou OSS):

- Situações da estrita responsabilidade da entidade responsável pela exploração e operação dos SI's da PTP (BSS e OSS) e que não tenham impacto na segurança de qualquer TI: bastará nestes casos a aprovação do Director responsável pela exploração e operação dos SI's na PTP;
   - Simetricamente, situações mais complexas que possam também pôr em causa, directa ou indirectamente, a segurança de TI's da PTP: para além da aprovação do Director responsável pela exploração e operação dos SI's na PTP, a excepção deverá ter adicionalmente a aprovação do Director responsável pela operacionalização e gestão dos serviços de TI's da PTP;

- No caso de excepções relativas ao Portal Sapo, bastará a aprovação do Director responsável pela tecnologia, engenharia e operação do Portal Sapo;

- No caso de excepções relativas à Rede Wireline da PTP, bastará a aprovação do Director responsável pela operação e manutenção da Rede Wireline devendo este, sempre que necessário, aconselhar-se junto das respectivas Direcções de Engenharia e da entidade responsável pela Política de Segurança da Informação da PTP;

- No caso de excepções relativas à Rede Wireless da PTP, bastará a aprovação do Director responsável pela operação e manutenção da Rede Wireless devendo este, sempre que necessário, aconselhar-se junto das respectivas Direcções de Engenharia e da entidade responsável pela Política de Segurança da Informação da PTP;

- Em caso de dúvida, deverá ser consultada a entidade responsável pela Política de Segurança da Informação da PTP;

A entidade responsável pela Política de Segurança da Informação procederá sempre que considere necessário, ao controlo das excepções documentadas e registadas. A informação das mesmas é um *input* essencial para o Processo de Gestão de Risco dos SI's/TI's da PTP, o qual é da sua responsabilidade, de acordo com o Manual de Controlo Interno.

Nota Importante:

As Direcções responsáveis pela concretização de novos projectos na PTP, que venham a resultar em novas aplicações ou novos sistemas e tecnologias de informação e comunicação, são igualmente responsáveis por garantirem o cumprimento integral da Política de Segurança da Informação da PTP. Em particular, é importante avaliar logo em fase de projecto o nível de segurança que uma nova solução deva ter. Por exemplo, caso seja provável que uma nova aplicação ou um novo sistema venha a ter impacto directo no relato financeiro da PTP, deve ser consequentemente considerado provável que esse sistema venha a ser no futuro incluído no âmbito do SOX, pelo que as respectivas implicações em matéria de segurança deverão de ser consideradas. Corrigir lacunas de segurança *a posteriori* é sempre uma proposição mais cara do que resolvê-las em fase de projecto.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

6.1 Internal Organization

8.2 Os Sistemas e Tecnologias já existentes e incluídos no âmbito SOX

Para os Sistemas e tecnologias já existentes e incluídos no âmbito SOX, em que se verifiquem situações em que a Política de Segurança da Informação não seja aplicável por razões técnicas e/ ou funcionais, as excepções, deverão ser documentadas e sujeitas a parecer da entidade responsável pela Política de Segurança da Informação, acompanhada de proposta de medidas que possam, entretanto, mitigar os riscos em causa.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

6.1 Internal Organization

8.3 Sistemas e Tecnologias já existentes e não incluídos no âmbito SOX

Para os Sistemas e tecnologias já existentes e não incluídos no âmbito SOX, é da responsabilidade da equipa responsável por esse sistema ou tecnologia a identificação da excepção, devendo a mesma excepção encontrar-se documentada e registada na CMDB respectiva ou, na falta desta, em meio equivalente. Sempre que uma acção de renovação tecnológica não conduza ao cumprimento integral da "*Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações*", deverá ser mantida a identificação deste sistema como uma excepção documentada, salvaguardando que nenhuma alteração

possa conduzir a uma situação de risco acrescido de segurança comparativamente à situação anteriormente em produção.

A entidade responsável pela Política de Segurança da Informação procederá periodicamente, e sempre que considere necessário, ao controlo das excepções documentadas e registadas. A informação das mesmas é um *input* essencial para o Processo de Gestão de Risco dos SI's/TI's da PTP, o qual é da sua responsabilidade, de acordo com o Manual de Controlo Interno.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

6.1 Internal Organization

8.4 Comunicação de Incidentes de Segurança

Sempre que seja identificada uma situação anómala que possa estar relacionada com a segurança lógica das TI's, SI's ou REDE da PTP, esta deve ser imediatamente comunicada ao CSIRT da PTP através dos seguintes pontos de contacto:

- Pelo CSI Atendimento (csi-atendimento@telecom.pt) que, após identificação rigorosa do seu interlocutor, fará o encaminhamento do incidente para o CSIRT da PTP;
- Por e-mail para o seguinte email: CSIRT@TELECOM.PT

A equipa do CSIRT deverá classificar os incidente em quanto à sua incidência, i.é.:

➔ incidente sobre TI's,

➔ incidente sobre SI's,

➔ incidente sobre áreas ligadas às Redes Wireline ou Wireless,

de seguida avaliar o risco envolvido no incidente comunicado e verificar a autenticidade do seu comunicante original, após o que deverá tentar resolvê-lo caso seja capaz, i.e., caso já conheça esse tipo de incidente, bem como a solução ou processo de mitigação recomendado.

Caso o incidente seja novo ou complexo, deverá encaminhá-lo imediatamente para a entidade responsável pela investigação do mesmo:

- **Incidentes associados a TI's**: para a entidade responsável pela operacionalização e gestão dos serviços de TI's da PTP;
- **Incidentes associados a SI's**: para a entidade responsável pela Política de Segurança da Informação da PTP;

- **Incidentes associados à REDE Wireline**: para a entidade responsável pela operação e manutenção da Rede Wireline, devendo esta, sempre que necessário, apoiar-se nas respectivas Direcções de Engenharia e entidade responsável pela Política de Segurança da Informação da PTP;
- **Incidentes associados à REDE Wireless**: para a entidade responsável pela operação e manutenção da Rede Wireless, devendo esta, sempre que necessário, apoiar-se nas respectivas Direcções de Engenharia e entidade responsável pela Política de Segurança da Informação da PTP;

Estas entidades deverão depois proceder ao registo do incidente numa base de informação segura do CSIRT, concebida para o efeito, e onde também deverá registar as acções de resolução ou mitigação empregues e seus resultados. Sempre que tal faça sentido, o conhecimento adquirido deverá ser passado à equipe do CSIRT.

A entidade responsável pela Política de Segurança da Informação procederá periodicamente, e sempre que considere necessário, ao controlo de todas as excepções documentadas e registadas. A informação relativa a estas excepções é um *input* essencial para o Processo de Gestão de Risco dos SI's/TI's da PTP, o qual é da responsabilidade da entidade responsável pela Política de Segurança da Informação, de acordo com o Manual de Controlo Interno.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

13.1 Reporting information security events and weaknesses

9 Revisão/ Actualização da Política de Segurança da Informação

9.1 Entidade responsável pela Política de Segurança da Informação

A entidade responsável pela Política de Segurança da Informação fará proposta ao Conselho de Administração da PTP (CA PTC, CA TMN, CA PT Prime) de revisão e actualização da Política sempre que a evolução tecnológica ou os dados históricos da organização o justifiquem, ou quando, para fazer face a exigências Legais Nacionais e/ ou Internacionais, seja imperativo a transcrição da mesma para a "Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações".

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

5.1.2 Review of the information security policy

9.2 Conselho de Administração da PTP (CA PTC, CA TMN, CA PT Prime)

O Conselho de Administração da PTP (CA PTC, CA TMN, CA PT Prime) efectuará alterações à "*Política de Segurança da Informação da PT Portugal (PT Comunicações, Tmn e PT Prime) a nível dos Sistemas e Tecnologias de Informação e Comunicações*" sempre que o considere necessário.

ISO / IEC 17799:2005 – Information Technology – Code of practice for information security management

5.1.2 Review of the information security policy

10 Glossário

A

Audit Trail **–** Trata-se de um *log* que de uma forma cronológica regista a sequência de eventos auditáveis, contendo evidência da execução de transacções ou funções de sistema. O mesmo deve conter informação relativa a: *"Quem fez?"*, *"O que fez?"*, *"Quando fez?"*, devendo guardar o valor/ parâmetro anterior e novo.

B

Base de dados – Conjunto de dados logicamente ligados entre si, num suporte que permite armazenamento de grande quantidade dos dados e geridos por um programa especializado denominado Sistema de Gestão de Bases de Dados. Este programa encarrega-se de armazenar e pesquisar os dados, garante independência entre a estrutura de armazenamento e outros programas que utilizam os dados, garante a segurança no acesso aos mesmos e assegura redundância e tolerância a falhas dos programas de consulta.

Biometria – É uma tecnologia de segurança baseada no reconhecimento de uma característica física, única e intransmissível das pessoas, como por exemplo, a impressão digital e a íris.

Bot (roBOT) **–** Programa que funciona como um agente para um Utilizador ou outro programa e simula actividades pré-programadas.

BotNet (roBOT NETwork) **–** É um grande número de computadores comprometidos, com *bots* instalados que executam actividades pré-programadas, muitas vezes controladas em tempo real, por um ou mais computadores na Internet (Bot Controllers).

BSS **–** *Business Support Systems*

C

Caderno de Encargos – Documento interno da PTP, elaborado pelo Cliente Interno PTP, no âmbito de determinada Consulta ao Mercado, que contém informação de negócio necessária e suficiente, especificações técnicas e/ou requisitos do Produto/Serviço identificado, bem como outras informações relevantes, e que será disponibilizado ao Fornecedor PTP para servir de base à respectiva elaboração da resposta a um RFI, RFQ ou RFP.

Chain Letters / Chain e-mails

Chave de cifra (*Encryption Key*) – Conjunto de *bytes* utilizados para controlo do algoritmo do processo de cifra.

Chave de cifra simétrica – O mesmo conjunto de *bytes* é utilizado para cifrar e decifrar os dados.

Cifrar (*Encryption*) – Processo que envolve a codificação de dados de forma

a garantir a confidencialidade, autenticidade, anonimato, "*time-stamping*" e outros objectivos de segurança.

Cliente interno – As pessoas, unidades operacionais, sociedades ou serviços, do grupo PT, que recorrem a outras unidades operacionais, sociedades ou serviços dentro da estrutura da PTP.

CMDB – Configuration Management Database

***Content Filter* –** É um automatismo que permite bloquear o acesso a sites ou a recepção de emails baseado na análise dos conteúdos envolvidos, prevenindo situações de *spam*, vírus, *worms*, *denial-of-service attacks*, *trojans*, *spyware, malware, pornografia, etc*. Vulgarmente, é utilizado em ambientes internet filtrando *emails* (ficheiros anexos a *emails*) e acessos a sites na internet que apresentem riscos de segurança.

Controlo de Acessos – Sistema que restringe as actividades dos Utilizadores e processos baseado no que é estritamente necessário saber/fazer. Permite implementar a segregação de funções.

D

Dado – Representação de um facto, medição, conceito ou ideia através da utilização de letras, números, caracteres especiais, imagens ou sons e armazenado num computador permitindo a sua posterior consulta, transmissão ou processamento usando meios informáticos.

Dados Pessoais – Qualquer informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. (*Lei 67/98 de 26 de Outubro* – Lei da Protecção de Dados Pessoais, alínea a) do artigo 3º).

Data Center – Local com as condições ambientais e técnicas, (incluindo de segurança física e lógica, adequadas ao alojamento de equipamentos / sistemas e onde existe um rigoroso controlo de acessos físicos e lógicos.

Directórios – Unidades organizacionais, utilizados para organizar ficheiros ou outros directórios que se encontram abaixo da sua hierarquia.

DMZ (*Demilitarized Zone*) – É um perímetro de segurança físico ou lógico utilizado para colocar "*front-ends*" dos serviços da empresa que se pretendem expor a um maior e não necessariamente confiável público-alvo, normalmente na Internet.

DoS (Denial of Service) e DDoS (Distributed Denial of Service) – Tipo de ataque a um sistema de informação ou rede com a intenção de provocar a indisponibilidade do serviço aos restantes Utilizadores, normalmente através da perda de conectividade e serviços pelo consumo agressivo da largura de banda da rede atacada ou de sobrecarga dos

recursos dos sistemas atacados. Designa-se DDoS quando o ataque envolve múltiplos sistemas, distribuídos na Internet.

E

Empresa Estendida – Ambiente alargado de uma empresa, tendo em conta as infra-estruturas dos seus parceiros, quando estas se tenham de interligar às suas próprias infra-estruturas para prestarem os seus serviços. Esta realidade estendida tem de ser tida em conta na análise global da segurança da informação de uma empresa.

Estação de Desenvolvimento (TD) – Computador pessoal, fixo e ou portátil, e respectivo software, disponibilizado pela PTP a um grupo restrito de Utilizadores, para uso profissional na PTP, ficando estes com privilégios de administração local do equipamento.

Estação de Trabalho (ET) – Computador pessoal, virtual (VDi), fixo e ou portátil, e respectivo software, disponibilizado pela PTP à maioria dos Utilizadores, para uso profissional na PTP, ficando estes sem qualquer privilégio de administração local do equipamento.

F

***File Share* Públicos, Privados** – São espaços em disco, para partilha de ficheiros para um número restrito de Utilizadores (Privados), ou para toda a rede em que se encontram (Públicos).

Firewall – Barreira lógica que tem como objectivo impedir que Utilizadores ou processos acedam para além de um determinado ponto da rede, sem que tenham previamente passado uma validação de segurança (exemplo, fornecer uma *password*).

FTP – File Transfer Protocol

H

http/https – Protocolos de comunicação da *World Wide Web, sendo o https a versão mais segura e recomendada para aplicações Web/Intranet envolvendo informação classificada ou sensível*;

I

IDS (*Intrusion Detection System*) – Sistema de detecção de intrusões ou de tentativas de intrusão.

IPS (*Intrusion Prevention System*) – Sistema de prevenção de intrusões.

Informação Confidencial – Designação do nível de sensibilidade da informação, cuja distribuição provocará danos expectáveis na PTP ou em empresas relacionadas; Os graus de classificação de segurança da informação definidos na PTP são os seguintes[14]:

- **PT Muito Secreto**
- **PT Secreto**
- **PT Confidencial**
- **PT Reservado**

[14] Ordem de Serviço 001403CE (PT SGPS) – Matérias Classificadas PT, Preparação, Manuseamento, Arquivo e Destruição. Entrada em vigor em de 01.08.2003

A descrição do significado de cada classificação poderá ser encontrada no ponto 5.1.

Interlocutor Autorizado – Colaborador PTP com competências atribuídas ou delegadas para a aprovação de pedidos de acessos e/ou pedidos de resolução de incidentes e/ou pedidos de alterações.

L

Load balancer – Técnicas e/ou soluções que permitem distribuir carga de trabalho pelos recursos em causa. Os recursos podem ser categorizados da seguinte forma: Storage, Rede ou CPU.

M

Malware – Refere toda a classe de software malicioso (vírus, spyware, worms, …) desenhado para se infiltrar no computador, tirando partido de vulnerabilidades de segurança, sem o consentimento do Utilizador, e que normalmente persegue objectivos ilícitos e/ou nocivos.

N

NDA[15] – *Non Disclosure Agreement (Acordo de confidencialidade)*

Networking **–** Série de pontos ou nós (computadores, activos de rede, impressoras, etc) interligados por um meio de comunicação (cabo de cobre, óptico, *wireless*, etc).

Network TAP's **–** Dispositivo de hardware que possibilita o acesso aos dados que passam na rede de comunicação entre computadores.

O

OSS **–** *Operational Support Systems*

P

Password – Conjunto secreto de caracteres utilizado para identificar um Utilizador ou um processo.

Password "default" ou Password de *"fábrica"* – *Password* inicial atribuída quando um novo Utilizador é criado ou *password* inicial disponibilizada por um fornecedor de hardware/software.

Plataforma de Serviços **–** são normalmente plataformas técnicas que permitem a disponibilização de funcionalidades associadas à parametrização de qualquer tipo de serviços nas redes – cobre, fibra, etc (criar/ activar/ desactivar, controlar sessões, protocolos, etc.)

Pólos Técnicos – Trata-se de instalações técnicas com acesso controlado, localizadas em edifícios normais da PTP, fora dos Datacenters, onde se encontram equipamentos de suporte aos Sistemas de Informação e Tecnologias de Comunicação, tipicamente com funções locais à zona da rede onde se encontra.

Privilégio – Capacidade autorizada de efectuar uma certa acção num sistema.

[15] De acordo com minuta a solicitar à Direcção Jurídica

Protocolos Seguros – conjunto de regras standard para a comunicação segura de dados através de um canal de transporte

R

Remote Shell – um programa informático que permite aceder remotamente a outro computador. O recurso a *remote shells* terá lugar nos termos e requisitos estritos desta Política.

RFI – *Request for Information* – Consulta ao Mercado para obtenção apenas de informação técnica relativa a determinado Produto/Serviço.

RFQ – *Request for Quotation* – Consulta ao Mercado para obtenção de informação técnica e comercial relativa a determinado Produto/Serviço.

RFP – *Request for Proposal* – Consulta ao Mercado para obtenção de proposta técnica e comercial relativa a determinado Produto/Serviço.

Rede *Wireless* – Uma rede *wireless* (sem fios) é uma rede de computadores que não necessita de ligações por cabos – sejam eles telefónicos, coaxiais ou ópticos — recorrendo a equipamentos que usam radiofrequência (*comunicação via ondas de rádio*) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.

Router **–** executa o roteamento do tráfego de rede. Os **Core Router** – são os *routers* que se encontram localizados nos *backbone* ou centros nevrálgicos da rede.

S

SCP – *Secure Copy Protocol*

SFTP – *Secure File Transfer Protocol*

Sistema Crítico – Para efeitos desta Política de Segurança, são considerados sistemas críticos aqueles sistemas onde um acesso não autorizado, ou a execução de uma operação não autorizada, pode originar um impacto financeiro negativo na organização.

SMTP – Simple Mail Transport Protocol

***Sniffer's* Passivos e Activos** – Programa que monitoriza e analisa tráfego de rede passivamente, sem causar qualquer intervenção na comunicação, ou activamente provocando interacção na comunicação e forçando os restantes sistemas a responderem à acção iniciada pelo *sniffer*.

***SNMP* – Simple Network Management Protocol**

SOC – *Security Operations Center*

***SpyWare* e SpyWare Bots** – Software infiltrado num computador que recolhe informação de uma organização ou pessoa sem o seu conhecimento e a transmite de um outro computador, normalmente na Internet. Um SpyWare Bot é um SpyWare mais sofisticado controlado por computadores remotos na Internet (Bot Controllers).

Sondas de Rede (*Network Probes*) – Computadores com capacidade de capturar e analisar tráfego de rede.

SOX – Sarbanes-Oxley – A lei Sarbanes-Oxley resultou das iniciativas do Senador Paul Sarbanes, presidente do Comité Bancário do Senado Americano, e do Congressista Michael Oxley. A lei foi aprovada em Julho de 2002 por ambas as câmaras legislativas Americanas, o Senado e o Congresso. O seu objectivo é reforçar as regras de controlo interno da informação financeira divulgada pelas empresas, de forma a restaurar a confiança nos mercados financeiros, abalada pelos escândalos financeiros da Enron, WorldCom, Tyco, entre outros.

Spam – *email* não solicitado primariamente com objectivos publicitários, enviado em grandes quantidades para indivíduos, listas, grupos, etc**.**

SSH **–** *Secure Shell*

Strong Authentication – Também designado T-FA (*Two-factor authentication*) é um protocolo de autenticação que requer duas formas de autenticação para aceder a um sistema, em que a 1ª forma de autenticação corresponde a algo que o Utilizador conhece (exemplo, um PIN ou uma *password*) e a 2ª forma corresponde a algo que o Utilizador possui (exemplo, cartão magnético ou impressão digital).

Switch de Rede **–** Comutador de rede

T

Time Stamping – é o processo de garantir de forma segura o registo do tempo de criação e modificação de um documento.

Túneis *(Tunneling)* – Tecnologia que permite encapsular pacotes de um protocolo em pacotes de um outro protocolo. Existem túneis para estabelecer comunicações mais seguras quando o protocolo envolvente permite encriptação. Existem também túneis criados para dissimular comunicações com protocolos proibidos numa organização encapsulando-os em protocolos comuns como https. Esta última utilização é estritamente proibida na PTP.

U

USB *Storage* – Dispositivo de armazenamento que se liga a uma porta USB (*Universal Serial Bus*).

Utilizador final – Elemento que usa um computador para suportar as actividades de negócio da PTP e que actua como a fonte ou destino da informação que fluí sobre um sistema de informação ou rede.

V

VDi (*Virtual Desktop Infrastructure*) – Estação de trabalho baseada num ecrã, teclado e rato mas estando o seu processamento entregue a uma máquina virtual que corre centralmente num servidor em ambiente de Datacenter.

Vírus – Programa que se replica, copiando-se para o código de outro programa, sistema de arranque do computador ou documento, e que normalmente persegue objectivos ilícitos e/ou nocivos.

W

***Worm* –** Programa que se replica para outros computadores através de falhas de segurança e essencialmente via rede de comunicação.

World Wide Web *(WWW)* – Sistema de servidores Internet que suportam documentos formatados em HTML (*HyperText Markup Language*). Espaço de informação no qual os recursos são identificados por identificadores globais denominados *Uniform Resource Identifiers* (URI).